Student IT/EE Workshop 2025

Report of Contributions

https://indico.global/e/10042

Contribution ID: **1** Type: **Poster**

Perception manipulation and subjective reception of data

Thursday 24 April 2025 11:30 (30 minutes)

The aim of this paper is to provide insight into how
the recipients'opinions may be manipulated in data visualization
scenarios. To obtain trustworthy and representative results, the
study involved an experiment, in which participants solved tasks
with charts that were purposefully modified to alter their perception of the data. The results indicate that this type of unethical
action can be effective, occasionally causing over 40% of the
recipients to be wrong or confused. Despite the limitations such
as a low number of participants, the observations made during
this study can be interpreted as a warning that misinformation is
a real threat. More research should be carried out to provide the
tools and information necessary to raise public awareness even
further.

Author: HORST, Filip

Presenter: HORST, Filip

Session Classification: Session C (Poster)

Contribution ID: **2** Type: **Poster**

Accelerating AI Inference in the Browser with WebGPU: Evaluating Quantization Trade-offs in Latency, Quality, and Memory Usage

Thursday 24 April 2025 10:45 (30 minutes)

Recent advances in deep learning and natural language processing have spurred the demand for deploying increasingly complex models on resource-constrained platforms. Modern browser environments, empowered by emerging GPU standards like WebGPU, now offer a promising venue for real-time AI inference. This paper provides an overview of leveraging WebGPU for accelerating inference directly within the browser, with a focus on evaluating the trade-offs associated with various quantization schemes. Our study examines the impact of quantization on inference latency, model quality, and memory usage across several model variants. Preliminary benchmarks demonstrate that carefully applied quantization can substantially reduce resource demands while maintaining acceptable performance, laying the groundwork for further optimization of browser-based AI applications. This work sets the stage for future explorations aimed at refining quantization techniques and expanding the capabilities of WebGPU-driven inference.

Authors: Mr RUSZPEL, Ignacy (Politechnika Warszawska - Wydział Elektryczny); Mr WÓJCIK, Nikodem (Politechnika Warszawska - Wydział Elektryczny)

Presenters: Mr RUSZPEL, Ignacy (Politechnika Warszawska - Wydział Elektryczny); Mr WÓJCIK, Nikodem (Politechnika Warszawska - Wydział Elektryczny)

Session Classification: Session B (Poster)

Contribution ID: **3** Type: **Poster**

BBot - Behavioral reinforced learning bot to play blood bowl

Thursday 24 April 2025 11:30 (30 minutes)

This paper presents a comparative study of different neural network architectures trained using behavioral learning in the strategic board game Blood Bowl. The game's complexity, driven by its large branching factor and inherent randomness, presents a significant challenge for artificial intelligence (AI). Traditional AI approaches, such as scripted and search-based methods, have struggled to achieve human-level performance. This study examines how various deep learning models process decision data, adapt strategies, and handle uncertainty in gameplay. Our methodology involves training models with a custom preprocessing pipeline that extracts valid game states and actions from replays of scripted solutions and tournament self-play. Performance is evaluated by competing against existing AI solutions, using metrics such as win rates, move efficiency, and strategic accuracy. The results highlight the comparative strengths and weaknesses of each architecture, providing insights into their effectiveness for reinforcement learning-based agents in complex decision-making environments like Blood Bowl.

Authors: NOWICKI, Bartosz; KOCIOŁEK, Karol; WOŁEK, Wiktor

Presenters: NOWICKI, Bartosz; KOCIOŁEK, Karol; WOŁEK, Wiktor

Session Classification: Session C (Poster)

Contribution ID: **4** Type: **Poster**

Comparison of multiplatform technologies for mobile application development

Thursday 24 April 2025 11:30 (30 minutes)

This paper compares technologies used to develop mobile applications using multiplatform technologies. A lack of analysis of newer technologies, such as Kotlin Multiplatform, was identified by researching the current state of this field. Therefore, this study aims to compare the Kotlin Multiplatform with existing and well-researched Flutter technology to advance mobile development techniques. A comparison has been drawn from both literature and practice.

Author: ANKIERSZTAJN, Michał

Presenter: ANKIERSZTAJN, Michał

Session Classification: Session C (Poster)

Contribution ID: **5** Type: **Poster**

Attacks on LSTM-Based Recurrent Neural Networks for Sentiment Analysis

Thursday 24 April 2025 11:30 (30 minutes)

Recurrent Neural Networks (RNN) and their other variants such as Long-Short Term Memory (LSTM) networks have become a widely used tool for natural langague processing (NLP). Thanks to their ability to effectively capture sequential dependencies in textual data they are well-suited for determining sentiment expressed in user-generated data such as media posts or reviews. However despite their effectiveness we cannot forget about their vulnerability for intentional perturbations in the input data possibly affecting their classification capabilities. This work is aimed to analyze impact of such manipulations on LSTM and non-LSTM based networks. The analysis was conducted on custom-made RNNs trained on database containing game reviews on Twitter. Research will involve specificaly two types of input data manipulations - synonymization and token replacement with the most semantically similar vectors. This work presents the effects of experiments comparing the aforementioned networks' resilience to perturbations and the way they affect model's classification abilities. Final findings suggest that LSTM models exhibit greater resistance to subtle input changes (using synonyms) than standard RNNs but remain susceptible to more advanced attacks (vector replacement). This study highlights the importance of research in domain of neural networks' security and opens new paths for future study in this direction.

Author: Mr ZAN, Rafał (Politechnika Warszawska)

Presenter: Mr ZAN, Rafał (Politechnika Warszawska)

Session Classification: Session C (Poster)

Contribution ID: **6** Type: **Presentation**

Convolutional Kolmogorov Arnold Networks as an accurate alternative to Convolutional Neural Networks for rule discovery in Game of Life

Thursday 24 April 2025 09:42 (12 minutes)

The interpretability of artificial neural networks (ANNs) remains a challenge, particularly as they grow deeper and incorporate millions of parameters. Kolmogorov-Arnold Networks (KANs) address this issue by using fewer parameters than traditional ANNs and representing functions as symbolic formulas, while maintaining comparable performance.

John Conway's Game of Life (GoL) serves as an example of reverse-engineering the rules underlying simple natural processes. We trained several networks, including KANs, Convolutional KANs (CKANs), and traditional Convolutional Neural Networks (CNNs), on a dataset of GoL-generated images and compared the learned kernels with expected ones.

Our findings show that both CKANs and CNNs can recover the rules of simple processes like GoL while validating model performance against traditional CNNs.

Authors: MICHALSKI, Maciej (Student); Mr FERENC, Patryk (inżynier); Mr GÓRKA, Sebastian (inżynier)

Presenters: MICHALSKI, Maciej (Student); Mr FERENC, Patryk (inżynier); Mr GÓRKA, Sebastian (inżynier)

Session Classification: Session A (Presentation)

Contribution ID: **7** Type: **Poster**

User experience laws: a literature review and practical examples based on DoorCE project

Thursday 24 April 2025 11:30 (30 minutes)

The article presents a detailed literature review on the topic of user experience design principles. The study synthesizes knowledge from research papers and books, focusing on user experience laws that can be applied while designing user interfaces.

The review highlights sources about Gestalt psychology in user experience design. The studied literature also emphasizes the importance of Miller's Law and Hick's Law regarding the complexity and Fitt's Law related to efficient layouts. Moreover, articles discussing navigational patterns such as Z-pattern and F-pattern are analyzed. In addition, sources on methods of increasing user interface accessibility are examined. Lastly, the article summarizes findings about consistency as a crucial element of user experience.

Based on the reviewed literature, the author presents practical examples. Examples come from two user interface prototypes of the DoorCE project –a joint initiative of many Central European institutions to make public data more accessible. These user interfaces are evaluated based on described laws and corrections are made where necessary. The result of this research is a set of design principles based on the current state of the art, each with its own example from a professional application.

Author: BALCER, Jerzy

Presenter: BALCER, Jerzy

Session Classification: Session C (Poster)

Contribution ID: **8** Type: **Poster**

Overview of Communication Mechanisms Adopted in Modern Systems

Thursday 24 April 2025 11:30 (30 minutes)

Abstract—In modern software systems, efficient communication is essential for ensuring scalability, maintainability, and performance. The aim of this article is to review key communication mechanisms used in modern systems. A multi-stage selection process was conducted to identify the most relevant scientific articles, summarize research findings, and determine which methods perform best in specific contexts. The search was carried out using selected electronic databases of scientific publications. Research indicates that REST is widely used and performs well, GraphQL is effective for retrieving large datasets, and gRPC enables fast data transfers. Additionally, Kafka, MQTT, and AMQP are the most suitable protocols for handling messaging in high-load distributed systems. The study emphasizes that choosing the right communication method is crucial and should consider specific system requirements such as data volume, speed, security, and the type of operations involved.
Index Terms—REST, SOAP, GraphQL, gRPC, AMQP, MQTT, Kafka, comparative overview

Authors: SZCZYGIELSKI, Jakub; ŻDANUK, Michał

Presenters: SZCZYGIELSKI, Jakub; ŻDANUK, Michał

Session Classification: Session C (Poster)

Contribution ID: **9** Type: **Poster**

Development of a model of the electric field distribution inside the human brain

Thursday 24 April 2025 11:30 (30 minutes)

This study focuses on optimizing the computational efficiency of simulating electric field distribution in the human brain using the finite element method (FEM). Due to the brain's complex and heterogeneous structure, accurate modeling requires high-resolution segmentation and realistic electrical property assignments, leading to large-scale numerical problems. To address these challenges, this research explores advanced numerical solvers, parallel computing strategies, and memory-efficient algorithms to enhance performance without compromising accuracy. Special attention is given to optimizing matrix assembly, preconditioning techniques, and load balancing in parallel computations, enabling faster convergence and reduced memory consumption. This study also investigates the performance of algebraic multigrid solvers, including the Ruge-Stuben AMG and Smoothed Aggregation AMG methods, to efficiently handle the large, sparse linear systems arising from FEM simulations. Additionally, we implement parallelized matrix assembly in Julia using distributed computing and shared memory techniques to optimize workload distribution and reduce communication overhead in large-scale simulations.

Authors: Dr CHABER, Bartosz (Warsaw University of Technology); Mr TRUSIEWICZ, Konrad (Warsaw University of Technology); Mr GURYN, Mikołaj (Warsaw University of Technology); Ms GAIK, Zuzanna (Warsaw University of Technology)

Presenters: Mr TRUSIEWICZ, Konrad (Warsaw University of Technology); Mr GURYN, Mikołaj (Warsaw University of Technology); Ms GAIK, Zuzanna (Warsaw University of Technology)

Session Classification: Session C (Poster)

Contribution ID: **10** Type: **Poster**

Enhancing Phishing Detection on Websites: A Hybrid Approach Combining Signature-Based Detection and Traditional Machine Learning Methods - Abstract

Thursday 24 April 2025 10:45 (30 minutes)

With the increasing popularity of web services and the significant amount of time users spend online, cybercriminals are increasingly targeting this space with sophisticated malicious techniques. Phishing, one of the most prevalent cybersecurity threats, poses a substantial risk to both individuals and organizations. These attacks are typically executed via deceptive emails containing fraudulent URLs that redirect users to malicious websites designed to steal sensitive information. The consequences of phishing can be severe, including financial loss, identity theft, and malware infections. To mitigate phishing threats, implementing an effective detection framework is essential. Existing detection techniques include signature-based methods, traditional machine learning models, and deep learning approaches. However, each method has inherent limitations, making it challenging to rely solely on a single technique. We propose a hybrid phishing detection approach that integrates signature-based detection with a machine learning model to enhance both versatility and robustness against phishing attacks. Email file in EML format works as an input to our solution which is later processed to extract hyperlinks from body of the message. Those URLs are then passed to signature-based detection component and machine learning model. The first component utilizes an API wrapper for the widely used cyber-threat intelligence platform. Meanwhile, the machine learning model is trained on feature extraction techniques using the open-source phishing URL dataset. Those features are based on URL attributes (e.g. domain length, HTTPS usage, number of special characters) and HTML attributes (e.g. number of hidden fields, redirections, JavaScript references). For the research purposes, we trained three different machine learning models: Decision Tree, MLP (Multi-Layer Perceptrons network), and SVM (Support Vector Machines). All of our models achieved an impressive accuracy of 0.9988, 0.9994, and 0.9982, respectively, demonstrating its effectiveness in identifying phishing threats. The results indicate that this hybrid approach can serve as a reliable cybersecurity tool, capable of detecting both existing and emerging phishing attacks with high precision.

Authors: ROMANEK, Jakub (Warsaw University of Technology); LATAWIEC, Marcin

Co-author: Dr CHABER, Bartek

Presenters: ROMANEK, Jakub (Warsaw University of Technology); LATAWIEC, Marcin

Session Classification: Session B (Poster)

Contribution ID: **11** Type: **Presentation**

Mamba SSM with Kalman Filtering in Pendulum RL environment

Thursday 24 April 2025 09:54 (12 minutes)

State-space models (SSMs) have emerged as a compelling alternative to Transformer architectures, delivering comparable performance at significantly lower computational cost. Although deterministic SSMs such as Mamba have achieved state-of-the-art results in areas like sequence modelling and image segmentation, their deterministic nature limits their suitability for probabilistic reinforcement learning (RL) environments, where uncertainty is intrinsic.

This paper introduces an architecture that integrates the Mamba SSM with the Kalman filter, enabling it to learn and adapt to uncertain environment dynamics. We validate the effectiveness of this approach on a modified Pendulum task from the Gymnasium RL library, demonstrating its potential for learning and representing complex dynamics in probabilistic settings.

Author: KLEPACKI, Piotr (Warsaw University of Technology)

Presenter: KLEPACKI, Piotr (Warsaw University of Technology)

Session Classification: Session A (Presentation)

Contribution ID: **12** Type: **Poster**

Comparative Analysis of Continuous Software Delivery Tools Using Github Actions and Jenkins as Examples

Thursday 24 April 2025 11:30 (30 minutes)

Continuous integration and continuous deployment (CI/CD) tools are fundamental to modern software development, enabling automated software delivery and deployment. While numerous CI/CD solutions exist, this study focuses on a comparative analysis of GitHub Actions and Jenkins, two widely used tools representing cloud-based and self-managed CI/CD solutions, respectively. The evaluation covers key aspects such as scalability, configuration complexity, integration capabilities, cost, stability, and resource consumption. Through empirical testing and case studies, the study examines their effectiveness in building, deploying, and testing software, as well as their ability to integrate with third-party platforms and optimize infrastructure usage. The results show that GitHub Actions offers seamless integration with the GitHub ecosystem, simplified setup, and cost-effective scalability, making it particularly suitable for small to mid-sized teams that rely on cloud-native workflows. Conversely, Jenkins offers extensive customization, advanced plugin support, and greater flexibility, making it the preferred choice for large enterprise environments requiring on-premises or hybrid infrastructure. This study highlights critical decision factors when choosing a CI/CD platform, including installation methods, infrastructure control, and long-term maintenance requirements. The findings contribute to a broader understanding of the trade-offs between cloud-native and self-managed CI/CD solutions, and provide insights applicable to evaluating other CI/CD tools in different development environments.

Author: PROKOPIUK, Paweł

Presenter: PROKOPIUK, Paweł

Session Classification: Session C (Poster)

Contribution ID: **13** Type: **Poster**

Wpływ stopnia sprzężenia klas na czas wprowadzenia zmian - badanie empiryczne

Thursday 24 April 2025 11:30 (30 minutes)

Zmiany w oprogramowaniu stanowią największą część kosztów ponoszonych podczas jego utrzymywania. Optymalizacja kosztów, a w szczególności czasu poświęconego na wprowadzanie zmian umożliwia organizacjom utrzymującym oprogramowanie uzyskanie przewagi konkurencyjnej. Kluczową aktywnością w modyfikacji kodu źródłowego jest jego zrozumienie, na co wpływ ma zastosowana struktura klas.
Prezentacja przedstawia eksperyment przeprowadzony na 10 programistach, przed każdym z nich postawiono dwa zadania dostosowania programu do nowych wymagań. Pierwsze zadanie stanowiło próbę kontrolną i obejmowało obszar wspólny dla obu wariantów programu. Zmierzony czas został wykorzystany jako baza normalizacji wyników badania w celu kontroli zmiennych zakłócających. Dla połowy z badanych kod źródłowy został zmodyfikowany metodą odwróconej refaktoryzacji, która zwiększyła metrykę sprzężenia *Message Passing Coupling* dwukrotnie w obszarze zadania drugiego.
Eksperyment został poprawnie przeprowadzony w 9 na 10 przypadków. Znormalizowany czas zadania drugiego wykazał 73% różnicę pomiędzy grupami, jednocześnie t test Welcha t = -3.23 p = 0.01 co ugruntowuje wynik jako statystycznie istotny.
Wyniki badania potwierdzają założenie praktyków, że w celu przyszłych oszczędności w obszarze dostosowywania oprogramowania programiści powinni utrzymywać sturuktury kodu o możliwie najniższym sprzężeniu klas. Jednocześnie wskazuje, że istotnym elementem poprawnego przeprowadzenia eksperymentu jest jednolity dostęp do informacji, a przyszłe próby odtworzenia powinny opierać się o większe grupy z zachowaniem niższych kosztów samego badania, wykorzystując technologię kontrolowanych środowisk programistycznych, używaną dziś w ocenie zdolności programistycznych (*Remote IDE*).

Author: PURA, Dawid (Revolut)

Presenter: PURA, Dawid (Revolut)

Session Classification: Session C (Poster)

Contribution ID: **14** Type: **Poster**

Przewidywanie wstrząsów wtórnych przy pomocy Sieci Neuronowych.

Thursday 24 April 2025 10:45 (30 minutes)

Silne trzesienia ziemi niosa ze soba ryzyko wystapienia wstrzas´ow wt´ornych, kt´ore moga powodowa´c wieksze zniszczenia ni˙z gł´owne trzesienie. Ze wzgledu na zło˙zono´s´c tego zjawiska oraz gwałtowno´s´c jego przebiegu, prognozowanie czasu wystapienia i intensywno´sci wstrzas´ow wt´ornych stanowi wcia˙z istotne wyzwanie dla sejsmologii. W niniejszym artykule zaprezentowano podej´scie do predykcji wstrzas´ow wt´ornych na podstawie analizy sejsmogram´ow gł´ownego zdarzenia. W tym celu zastosowano sieci konwolucyjne (CNN) oraz rekurencyjne (RNN) do budowy modeli predykcyjnych. Sieci konwolucyjne, wyspecjalizowane w rozpoznawaniu wzorc´ow, wykorzystano do identyfikacji trzesie ´n ziemi, kt´ore moga wywoła´c wstrzasy wt´orne. Umo˙zliwiaja one analize zar´owno w dziedzinie czasu –przy czym surowy sejsmogram stanowi bezpo´srednie wej´scie do sieci neuronowej –jak i w dziedzinie czestotliwo´sci, gdzie zastosowanie transformaty Fouriera pozwala uzyska´c widmo sejsmogramu. Dodatkowo, sieci rekurencyjne zostały u˙zyte do modelowania korelacji pomiedzy poszczeg´olnymi segmentami czasowymi. Proponowana metodologia zakłada optymalizacje całego systemu, majaca na celu zwiekszenie dokładno´sci przewidywania zjawisk wt´ornych przy jednoczesnym ograniczeniu liczby fałszywych alarm´ow. W dłu˙zszej perspektywie rozwiazanie to mo˙ze przyczyni´c sie do zwiekszenia bezpiecze ´nstwa ludno´sci oraz usprawnienia podejmowania decyzji dotyczacych organizacji akcji ratowniczych i planowania działa ´n prewencyjnych. Dalszy rozw´oj przedstawionego podej´scia planowany jest w kierunku zwiekszenia precyzji wykrywania słabszych zjawisk sejsmicznych Index Terms—trzesienie ziemi, wstrzasy wkt´orne, sztuczne sieci neuronowe

Author: KLĘBOWSKI, Mikołaj

Co-author: Dr BACZYŃSKI, Dariusz (Politechnika Warszawska)

Presenter: KLĘBOWSKI, Mikołaj

Session Classification: Session B (Poster)

Contribution ID: **15** Type: **Poster**

Explainability of Convolutional Neural Network: Overview of Methods

Thursday 24 April 2025 10:45 (30 minutes)

Understanding and interpreting the decisions made by deep learning models has become an essential area of research in artificial intelligence. Convolutional neural networks (CNNs), despite their high performance in various tasks, often function as "black boxes," making it challenging to explain their predictions. This study focuses on applying and evaluating different explainability techniques to CNN models to gain more insight into their decision-making processes. Using multiple approaches, our aim was to assess the effectiveness and reliability of these methods in improving the transparency and interpretability of neural networks.

Authors: KRUSZYŃSKI, Jan (PW); Mr SONBUL, Karim (PW); Mr MARKOWICZ, Magdalena (PW); Mr PODGÓRSKI, Piotr (PW)

Co-author: SIWEK, Krzysztof

Presenter: Mr MARKOWICZ, Magdalena (PW)

Session Classification: Session B (Poster)

Contribution ID: **16** Type: **Poster**

Evaluating detection methods of synthetic images

Thursday 24 April 2025 10:45 (30 minutes)

The paper aims to evaluate the effectiveness of available detectors in distinguishing fake from real photos. Deepfakes are artificially generated images or videos created using artificial intelligence or manual tools like Photoshop. New techniques, such as Generative Adversarial Networks (GANs) and Diffusion Models (DMs) enable the rapid generation of highly realistic images. The research utilizes the StyleGAN3 (GAN) and Stable Diffusion XL (DM) models, which were previously fine-tuned on photos of beaten people obtained from the Internet to generate new images. Tests of the detectors were carried out to assess the detector's precision, sensitivity, and resistance to manipulations, such as graphic filters or compression, as well as resistance to fingerprint removal tools. Older detectors that were not trained on the tested generative models struggle to detect fake photos. In contrast, newer detectors trained on new latest models achieve surprisingly good results. These results highlight the need for continuous updates to detection systems to counteract evolving deepfake generation techniques.

Authors: Mr WÓJTOWICZ, Michal (Warsaw University of Technology); BILIŃSKI, Michał (Warsaw University of Technology)

Presenters: Mr WÓJTOWICZ, Michal (Warsaw University of Technology); BILIŃSKI, Michał (Warsaw University of Technology)

Session Classification: Session B (Poster)

Contribution ID: **17** Type: **Poster**

Comparative Analysis of Multi-Agent LLM Systems for Solving Polish Matura in Physics Exams

Thursday 24 April 2025 10:45 (30 minutes)

Large Language Models have gained widespread
recognition since OpenAI released their revolutionary model,
ChatGPT 3.5. Since then, many new approaches have emerged
to improve the capabilities and accuracy of these models for
different tasks. One such method involves using multi-agent
conversations. This article compares two multi-agent setups
designed to solve the Polish standardized high school exam in
physics. Comparative benchmarks were performed on several
real final exams published by the Polish Central Examination
Board (pl. CKE —Centralna Komisja Egzaminacyjna). The
study employed ChatGPT-4 Turbo and the AutoGen framework.
Benchmarks covered a total of 90 tasks from three Polish Matura
physics exams (editions: 2018, 2019, 2023). The simpler multiagent systems achieved an average score of 76.1%, while the
more complex systems averaged 85.6%.

Author: WRÓBEL, Piotr (Politechnika Warszawska)

Presenter: WRÓBEL, Piotr (Politechnika Warszawska)

Session Classification: Session B (Poster)

Contribution ID: **18** Type: **Poster**

Flutter vs. React for Web Applications: A Comparative Benchmark Study of Performance Metrics and Developer Experience

Thursday 24 April 2025 11:30 (30 minutes)

Rapid growth in device types used for running applications created a need for tools that allow cross-platform development.
This paper aims to benchmark multiple metrics, such as build size and speed index, to determine if Flutter is a good choice for writing web applications. Additionally, this research analyzes developer experience factors to provide a comprehensive evaluation beyond performance metrics alone.
Results of the performed benchmark show that React is better in most of the chosen metrics. The build sizes of Flutter applications are multiple times bigger, affecting the time needed to load initial chunks when the user first enters the website. Flutter architecture requires it to load its render engine so that the user can see content in the browser. These findings suggest that while Flutter offers the benefit of a unified codebase, its current performance limitations on the web can hinder its adoption for production-grade applications. Despite Flutter's comprehensive documentation, the web-specific guidance was noticeably less mature than React's extensive community resources and well-established best practices for web development.

Author: Mr WITCZAK, Jakub

Presenter: Mr WITCZAK, Jakub

Session Classification: Session C (Poster)

Contribution ID: **19** Type: **Poster**

Examination of PCA Utilisation for Multilabel Classifier of Multispectral Images

Thursday 24 April 2025 10:45 (30 minutes)

This paper investigates the utility of Principal Component Analysis (PCA) for multi-label classification of multispectral images using ResNet50 and DINOv2, acknowledging the high dimensionality of such data and the associated processing challenges. Multi-label classification, where each image may belong to multiple classes, adds further complexity to feature extraction. Our pipeline includes an optional PCA step that reduces the data to three dimensions before feeding it into a three-layer classifier. The findings demonstrate that the effectiveness of PCA for multi-label multispectral image classification depends strongly on the chosen deep learning architecture and training strategy, opening avenues for future research into self-supervised pre-training and alternative dimensionality reduction approaches.

Authors: Mr STASZYNSKI, Bartosz (Warsaw University of Technology); Mr KARPOWICZ, Filip (Warsaw University of Technology); Dr SARWAS, Grzegorz (Warsaw University of Technology); KĘPIŃSKI, Wiktor (Warsaw University of Technology)

Presenters: Mr STASZYNSKI, Bartosz (Warsaw University of Technology); Mr KARPOWICZ, Filip (Warsaw University of Technology); KĘPIŃSKI, Wiktor (Warsaw University of Technology)

Session Classification: Session B (Poster)

Contribution ID: **20** Type: **Poster**

Post-Quantum Cryptography: Benchmarking ML-KEM Against RSA

Thursday 24 April 2025 10:45 (30 minutes)

The rise of quantum computing presents a significant threat to classical cryptographic systems, particularly those relying on hard mathematical problems such as integer factorization and discrete logarithms. This paper explores the impact of quantum computing on traditional cryptographic algorithms and the necessity of transitioning to quantum-resistant cryptography. We provide an overview of post-quantum cryptographic (PQC) algorithms newly standardized by the National Institute of Standards and Technology (NIST) in the Federal Information Processing Standards (FIPS) 203, 204, and 205, which define quantum-secure key encapsulation and digital signature schemes. We examine existing implementations of these algorithms and evaluate the performance of ML-KEM against its classical alternative – RSA. Our findings highlight the feasibility of deploying PQC in real-world systems by demonstrating that at high security levels, ML-KEM can achieve significantly faster operation speeds than RSA, proving its ability to provide both strong security and practical efficiency.

Authors: PACEK, Dominika (Warsaw University of Technology); ŁABĘCKA, Nina (Warsaw University of Technology)

Presenter: ŁABĘCKA, Nina (Warsaw University of Technology)

Session Classification: Session B (Poster)

Contribution ID: **21** Type: **Poster**

Analysis and comparison of missing value imputation methods for atmospheric pollution data

Thursday 24 April 2025 10:45 (30 minutes)

Missing values are a common phenomenon in real-world time series datasets and can significantly impact the precision and reliability of data analysis and machine learning models. This research project aims to discuss the types of missing data occurrence and test and analyze different possibilities of their imputation. The methods taken into consideration will start from the simplest ones based on statistics, go through regression models, neural networks, and finally LLMs.

The effectiveness of these imputation techniques will be measured and tested on atmospheric pollution data, primarily focusing on PM10, PM2.5, SO2, and NO2 levels. The performance of each method will be evaluated based on accuracy, consistency, and the impact on subsequent predictive models.

Author: JASIŃSKI, Jakub (Warsaw University of Technology)

Presenter: JASIŃSKI, Jakub (Warsaw University of Technology)

Session Classification: Session B (Poster)

Contribution ID: **22** Type: **Poster**

Badania i Implementacja Innowacyjnego Systemu Zasobnika Energii Współpracującego z Odnawialnymi Źródłami Energii INNOSTOR dla Zrównoważonego Rozwoju na Politechnice Warszawskiej

Thursday 24 April 2025 11:30 (30 minutes)

W artykule przedstawione zostały dotychczasowe postępy projektu *Badania i Implementacja Innowacyjnego Systemu Zasobnika Energii Współpracującego z Odnawialnymi Źródłami Energii INNOSTOR dla Zrównoważonego Rozwoju na Politechnice Warszawskiej* realizowanego przez koło naukowe IskIErka w ramach grantu rektorskiego. Opisany został ogólny kierunek zmian w elektroenergetyce, dążący do coraz większego udziału źródeł odnawialnych w miksie energetycznym. Omówiona została związana z tym zagadnieniem problematyka nadpodaży energii elektrycznej w KSE i niedopasowania krzywej generacji do krzywej obciążenia. Przedstawiona została perspektywa prosumenta jako uczestnika wspomnianych procesów. Zarysowano możliwe rozwiązania tych problemów, ze szczególnym uwzględnieniem lokalnych magazynów energii elektrycznej, współpracujących ze źródłami odnawialnymi, w ramach instalacji prosumenckich małej mocy. Zaprezentowano projekt układu oferującego optymalne warunki prowadzenia badań w tej tematyce. Omówiono kwestię doboru odpowiednich urządzeń wytwórczych i magazynów energii, wraz z ich parametrami. Przedstawiony został obecny postęp prac oraz zebrane dotychczas pomiary. Na ich podstawie wyciągnięte zostały pierwsze wnioski. Opisane zostały dalsze etapy realizacji projektu, a także jego końcowe cele i perspektywy.

Authors: Mr SADOWSKI, Adam (Politechnika Warszawska); Ms SZULC, Dorota (Politechnika Warszawska); Mr ĆWIEK, Jakub (Politechnika Warszawska); Mr KOWALIK, Jan (Politechnika Warszawska); Mr JĘCZMIENIOWSKI, Krzysztof (Politechnika Warszawska); Mr KUCHARSKI, Ryszard (Politechnika Warszawska)

Presenters: Mr ĆWIEK, Jakub (Politechnika Warszawska); Mr KOWALIK, Jan (Politechnika Warszawska); Mr KUCHARSKI, Ryszard (Politechnika Warszawska)

Session Classification: Session C (Poster)

Contribution ID: **23** Type: **Poster**

Comparative Analysis of Machine Learning and Statistical Models for Short-Term Energy Production Forecasting in Poland

Thursday 24 April 2025 10:45 (30 minutes)

This paper investigates short-term energy production forecasting in Poland using three distinct predictive models: LightGBM, an ARIMA-based model, and a Long Short-Term Memory (LSTM) network. Leveraging historical data from Poland's energy sector, our study evaluates each model's performance in terms of accuracy, robustness, and computational efficiency. The LightGBM model employs gradient boosting techniques to capture non-linear relationships, while the ARIMA approach provides a classical linear autoregressive approach. Meanwhile, the LSTM network exploits its recurrent architecture to model complex temporal dependencies inherent in the time-series data. Comparative analysis based on metrics such as RMSE and MAE demonstrates that although all models exhibit competitive forecasting abilities, the LSTM model exhibits a modest performance advantage over the other approaches within the examined forecast scenario. However, both the LightGBM and ARIMA models offer advantages in terms of reduced computational overhead and ease of implementation. Furthermore, I analyze ensemble models in search of the most accurate predictions. The insights derived from this analysis aim to assist policymakers and energy sector stakeholders in making informed decisions regarding energy distribution and operational planning in Poland.

Index Terms—energy forecasting, time series, machine learning, LightGBM, LSTM, ARIMA

Author: KARPIŃSKI, Jakub (Warsaw University of Technology)

Presenter: KARPIŃSKI, Jakub (Warsaw University of Technology)

Session Classification: Session B (Poster)

Contribution ID: **24** Type: **Presentation**

Procedural civilization development including economical aspects and the terrain.

Thursday 24 April 2025 09:30 (12 minutes)

This article presents the project's results, focused on the simulation of civilizations that develop over time. The development is primarily influenced by three main factors: the terrain on which the tribes are initially placed, available resources, and economic aspects, such as trading with one another. The world is generated using procedural techniques, which return a world with realistic terrain shape, temperature, wind and humidity. The tribes traverse the terrain in search of resources and a spot to settle down while also interacting with other tribes and taking different courses of action based on their behaviours and their history with each other. After settling down, the tribe begins to build a city, trying to provide housing and food to each of its members, becoming self-sufficient and creating a better environment for future growth. The cities are generated using procedural techniques, mainly L-systems, and develop over time, creating more advanced types of buildings (such as taverns and temples) while improving existing housing.

Authors: KOSTERA, Michał (Politechnika Warszawska student); CEGIELSKI, Paweł (Student)

Co-author: Dr HRYNIÓW, Krzysztof (Warsaw University of Technology)

Presenters: KOSTERA, Michał (Politechnika Warszawska student); CEGIELSKI, Paweł (Student)

Session Classification: Session A (Presentation)

Contribution ID: **25** Type: **Poster**

Spatio-Temporal Memory System for Robots: Enabling Long-Term Contextual Reasoning

Thursday 24 April 2025 11:30 (30 minutes)

Enabling robots to operate autonomously in dynamic environments over extended periods requires robust memory, reasoning, and decision-making capabilities. Although large language models (LLMs) have demonstrated significant potential, their limited context size constrains their ability to manage long-term data effectively. Autonomous systems must be able to provide detailed information about a robot's past actions, locations, and observations—critical for supporting human decision-making and ensuring reliable long-term operation.

To address this challenge, we introduce a Spatio-Temporal Memory System integrated into the RAI framework. This system enables robots to collect, organize, and reason over data accumulated over hours, weeks, or even months. By capturing and structuring spatial, temporal, and visual information, it allows robots to efficiently retrieve relevant data and respond to complex queries with high accuracy and speed.

The system operates through two parallel processes: memory construction and query execution. This design ensures continuous data collection while enabling real-time user queries. To facilitate scalable and efficient data retrieval, the architecture integrates vector databases and NoSQL storage. In addition, it supports multimodal data processing, location- and time-based indexing, and semantic search, significantly improving the ability of a robot to recall and reason about past experiences.

Real-world evaluations demonstrate the effectiveness of the system in improving autonomous decision making and long-term adaptability. This work presents a scalable and practical solution for robots that navigate complex and evolving environments. The implementation is open source and available at: https://github.com/RobotecAI/rai

Author: MAJEK, Maciej (Warsaw University of Technology)

Presenter: MAJEK, Maciej (Warsaw University of Technology)

Session Classification: Session C (Poster)

Contribution ID: **26** Type: **Poster**

Verification of the authenticity of bullion coins with a mobile application based on frequency analysis using an artificial neural network

Thursday 24 April 2025 10:45 (30 minutes)

Counterfeiting of bullion coins is a serious issue for collectors, dealers and investors, highlighting the need for reliable and accessible authentication tools. This research presents a mobile application designed to authenticate bullion coins using audio analysis, offering an innovative and convenient solution. The app uses autoencoders, a form of artificial neural network, trained on spectrograms created from audio recordings of real coins being struck. These spectrograms capture unique frequency patterns, which the neural network analyses to recognise the acoustic signatures of authentic coins. Tests show that the application achieves high accuracy in distinguishing genuine coins from counterfeits, advancing non-destructive authentication methods. It offers practical benefits by allowing users such as collectors and dealers to instantly verify coins without special tools, increasing confidence in transactions. However, the performance of the application relies heavily on the quality of the audio recording, which can be affected by background noise or device limitations. The training dataset, while detailed, may not yet cover all coin types or counterfeit variations, which could reduce its effectiveness in some cases. Future efforts should aim to improve the application by expanding the dataset and incorporating additional data, such as weight or visual checks, to improve accuracy and versatility.

Author: GRYCZKA, Tomasz

Presenter: GRYCZKA, Tomasz

Session Classification: Session B (Poster)

Contribution ID: **27** Type: **Poster**

Projekt uniwersalnego robota modularnego

Thursday 24 April 2025 11:30 (30 minutes)

Wersja polska

Celem pracy jest przedstawienie robota modularnego Gizmo - jego budowy mechanicznej, koncepcji rozproszonego układu sterowania oraz protokołu komunikacji międzymodułowej. Zawiera ona również omówienie fizycznego modelu wykonanego z użyciem druku 3D. Każdy z segmentów posiada niezależne aktuatory oraz zdolność do łączenia się i rekonfiguracji. Cechy te sprawią, że roboty modularne mogą przyjmować różne topologie pozwalające na realizację manipulatorów, robotów mobilnych czy kroczących. W ramach artykułu omówiono również potencjalne zastosowania rozciągające się od przemysłu do branży edukacyjnej.

English version

The objective of this work is to present the modular robot Gizmo, focusing on its mechanical design, the concept of a distributed control system, and the inter-module communication protocol. The paper also discusses the physical model constructed using 3D printing. Each segment of the robot is equipped with independent actuators and the ability to connect and reconfigure. These characteristics enable modular robots to adopt various topologies, facilitating the development of manipulators, mobile robots, or legged robots. Additionally, the article explores potential applications spanning across industries and the educational sector.

Authors: BRZEZIŃSKI, Feliks; Mr OLSZEWSKI, Kacper; Ms PŁODOWSKA, Patrycja

Presenters: BRZEZIŃSKI, Feliks; Mr OLSZEWSKI, Kacper; Ms PŁODOWSKA, Patrycja

Session Classification: Session C (Poster)

Contribution ID: **28** Type: **Poster**

HDR - the impact of input parameters on the result for Debevec algorithm

Thursday 24 April 2025 11:30 (30 minutes)

Humans can perceive a much broader luminance range than an average camera. It is impossible to take a single photo that contains details for both very dark and bright areas.

HDRI (High Dynamic Range Imaging) methods address that problem, by merging multiple low dynamic range images (LDR) into a single picture. These methods are being used for professional cameras and even in smartphones.

The purpose of this article is to examine the optimal input parameters, including, among others, the number of images, their exposure times, and weighting functions using the Debevec-Malik method.

The images were taken from various scenes. Each scene was captured multiple times (in RAW and JPEG format) with different exposure duration, but with constant sensitivity and aperture. The experimental setup featured a stationary Nikon D40 camera mounted on a tripod. Photos had to be taken in the shortest possible time to avoid problems caused by movement within the scene, including clouds and people.

Multiple combinations of input parameters were investigated to create HDR images for every scene. In this paper, the histograms of both the composite HDR images and their individual source frames were examined. In addition, HDR images were evaluated in terms of noise characteristics, color fidelity, and overall realism. Finally, the radiance map and the camera response curve were analyzed to provide detailed information on image quality and dynamic range.

Each additional photo with a different exposure provides new information about the scene, potentially improving image quality and reducing noise. However, as will be shown, there is no need to use an excessively high number of images, as the benefits diminish rapidly after a certain point. Therefore, a smaller number of images can be used, resulting in faster processing times.

This research could be further expanded by incorporating a light meter to compare the obtained measured values with calibrated HDR image radiances. Additionally, exploring different HDR imaging approaches, pixel selection methods, and weight functions could help refine and validate the proposed methods.

Authors: MACIEJEWSKI, Jakub (Warsaw University of Technology); ZIOBER, Michał (Warsaw University of Technology)

Presenters: MACIEJEWSKI, Jakub (Warsaw University of Technology); ZIOBER, Michał (Warsaw University of Technology)

Session Classification: Session C (Poster)

Contribution ID: **29** Type: **Poster**

Evaluating unsupervised data mining methods to assess the utility of such approaches for SIEM event analysis.

Thursday 24 April 2025 10:45 (30 minutes)

Modern organizations generate vast amounts of data, a significant portion of which consists of system, network, and application logs. The sheer volume and scalability of these logs make manual analysis inefficient and highly time-consuming. Automated anomaly detection techniques have been developed and refined to accelerate this process. Currently it is common for open SIEM systems to only support basic anomaly detection features. In our paper, we focus on unsupervised data mining methods for anomaly detection in time-series JSON data. This study compares and explores the utility of several anomaly detection algorithms applied to preprocessed data. The preprocessing stage includes time-bucket segmentation and feature extraction. We have also examined different approaches to preprocessing that are mentioned in the literature. Among the various methods, Isolation Forest and probabilistic algorithms like ECOD, have been proven to perform well on multidimensional semi-structured text datasets. Furthermore, we assessed the performance of selected methods using relevant Key Performance Indicators and compared them in different scenarios. Our findings suggest that some of these methods could be adapted to effectively support security analysts working with SIEM systems. Certain concepts developed within this proof-of-concept study could be further refined and integrated into a dedicated tool for log analysis.

Author: DYDO, Marcin (Warsaw University of Technology)

Presenter: DYDO, Marcin (Warsaw University of Technology)

Session Classification: Session B (Poster)

Contribution ID: **30** Type: **Poster**

Comparing the Efficiency of Selected Reinforcement Learning Algorithms in Stability Control and Navigation Tasks

Thursday 24 April 2025 10:45 (30 minutes)

This paper presents a comprehensive comparison of the efficiency of four key reinforcement learning algorithms (DQN, PPO, REINFORCE, and A2C) in stability control and navigation tasks. The study was conducted in two test environments: Cart Pole, representing a basic balance maintenance task, and Lunar Lander, constituting a complex navigational challenge requiring precise landing. As part of the research, the algorithms were implemented using various neural network architectures adapted to the specific requirements of each environment. For the Cart Pole environment, simpler architectures were applied, while for the more complex Lunar Lander environment, enhanced networks with additional learning process stabilization techniques were implemented, such as layer normalization and orthogonal initialization.

The research methodology focuses on a systematic analysis of key performance aspects, including convergence speed, sample efficiency, adaptability to different initial conditions, and learning process stability over time. For each algorithm and environment, standardized experiments were conducted with detailed performance metrics recorded throughout the training process. The experiments revealed significant differences in how algorithms perform under varying levels of environmental complexity.

The comparative analysis revealed significant differences between algorithms in terms of learning approach, training process stability, and ability to efficiently utilize accumulated experiences. These observations emphasize that selecting an appropriate algorithm strongly depends on the specifics of the particular task, environmental complexity, and available computational resources. This research provides practical insights into algorithm selection and configuration for reinforcement learning tasks of varying complexity in the domains of stability control and navigation.

Index Terms—reinforcement learning, deep Q-network, proximal policy optimization, REINFORCE, advantage actor-critic, stability control, navigation tasks, Cart Pole, Lunar Lander

Author: WYŁUCKI, Oskar

Co-author: Dr ROSZCZYK, Radosław (Wydział Elektryczny)

Presenter: WYŁUCKI, Oskar

Session Classification: Session B (Poster)

Contribution ID: **31** Type: **Poster**

A Lung Volume-Based Perfusion SPECT and CT Comparison Algorithm for Enhanced Pulmonary Embolism Diagnosis

Thursday 24 April 2025 10:45 (30 minutes)

I. BACKGROUND
Pulmonary Embolism (PE) is reported to be one of the most common cardiovascular diseases. It is caused by a blood clot that develops in a blood vessel elsewhere in the body and travels to an artery in the lung, forming a blockage [1].

Lung V/Q (ventilation/perfusion) SPECT is one of an established diagnostic imaging test for suspected PE. The idea behind this test is to administer patient the radioactive tracer intravenous or by inhalation and use a gamma camera to detect the radiation emitted. The regular CT is also often performed to improve diagnosis sensitivity and specificity [2].

II. PURPOSE
The goal is to develop an algorithm estimating lung volumes from Perfusion SPECT and CT examinations and calculate the ratio VP /VCT (Perfusion lung volume to CT lung volume). The assumption is that a low ratio may indicate the presence of regions with no perfusion, suggesting the patient may be suffering from PE. This algorithm may improve the sensitivity and specificity of PE diagnosis and introduces an automatically calculated metric quantifying the severity of potential PE.

III. MATERIALS AND METHODS
During our studies, we developed a method for calculating lung volumes using two complementary imaging modalities: SPECT and CT. Our dataset comprised 5 patients —3 diagnosed with Pulmonary Embolism (PE) and 2 healthy controls. Both scans were available for each patient, acquired through our collaboration with the Warsaw Military Institute of Medicine.

Data processing involved analysis of DICOM files containing both CT and SPECT images along with their associated metadata. For segmentation, we employed distinct approaches tailored to each modality: SPECT images were segmented using a standardized fixed threshold method, while CT images were processed using an established machine learning algorithm based on transfer learning of U-net architecture, implemented through the lungmask [3] library. We improved the CT segmentation process by converting pixel values to Hounsfield Units (HU) as a crucial preprocessing step. Lung volumes for both imaging modalities were calculated using the physical voxel dimensions from the image metadata. This dual-modality approach ultimately enabled us to calculate the Perfusion/CT ratio based on the segmented volumes.

IV. RESULTS

The developed algorithm successfully distinguished between PE-diseased and healthy patients. The maximum volume ratio observed in the diseased group was 0.695, while the minimum value in the healthy group was 0.869.

V. CONCLUSION
Although the algorithm effectively differentiated between the two groups, the limited sample size suggests the need for further research and additional data to validate the findings, determine a reliable threshold, and establish fundamental metrics such as sensitivity and specificity.

REFERENCES

[1] A. C. Clark, J. Xue, and A. Sharma, ‘Pulmonary Embolism: Epidemiology, Patient Presentation, Diagnosis, and Treatment’, Journal of Radiology Nursing, vol. 38, no. 2, pp. 112–118, Jun. 2019, doi: 10.1016/j.jradnu.2019.01.006.
[2] M. Bajc, J. B. Neilly, M. Miniati, C. Schuemichen, M. Meignan, and B. Jonson, ‘EANM guidelines for ventilation/perfusion scintigraphy: Part 1. Pulmonary imaging with ventilation/perfusion single photon emission tomography’, Eur J Nucl Med Mol Imaging, vol. 36, no. 8, pp. 1356–1370, Aug. 2009, doi: 10.1007/s00259-009-1170-5.
[3] J. Hofmanninger, F. Prayer, J. Pan, S. R¨ohrich, H. Prosch, and G. Langs, ‘Automatic lung segmentation in routine imaging is primarily a data diversity problem, not a methodology problem’, European Radiology Experimental, vol. 4, no. 1, p. 50, Aug. 2020, doi: 10.1186/s41747-020-00173-2.

Authors: Mr KISIEL, Daniel (Politechnika Warszawska); Mr MUCHOROWSKI, Eryk (Politechnika Warszawska); Dr ROSZCZYK, Radosław (Politechnika Warszawska)

Presenters: Mr KISIEL, Daniel (Politechnika Warszawska); Mr MUCHOROWSKI, Eryk (Politechnika Warszawska)

Session Classification: Session B (Poster)

Contribution ID: **32** Type: **Poster**

Porównanie wydajności i skuteczności algorytmów mieszających

W niniejszej pracy dokonano porównania wydajności i skuteczności różnych algorytmów mieszających ze szczególnym uwzględnieniem ich odporności na kolizje oraz szybkości obliczeniowej. Badanie przeprowadzono na platformie mobilnej, analizując historyczne oraz współczesne implementacje funkcji skrótu, takie jak MD5, SHA oraz BLAKE, w różnych wariantach. W pracy omówiono ich zastosowania, wady i zalety oraz wpływ architektury na efektywność działania. Wyniki testów pozwoliły na wyłonienie algorytmu, który oferuje optymalny kompromis między bezpieczeństwem a wydajnością obliczeniową.

Author: ZILINSKI, Konrad

Presenter: ZILINSKI, Konrad

Contribution ID: **33** Type: **Poster**

Przegląd znakowania wodnego obrazów we współczesnych zastosowaniach

Thursday 24 April 2025 11:30 (30 minutes)

Dynamiczny rozwój sztucznej inteligencji oraz mediów społecznościowych zwiększają potrzebę skutecznej ochrony przekazywanych danych. Znakowanie wodne jest jedną z możliwych technik modyfikujących m. in. obrazy w celu śledzenia przepływu informacji i pochodzenia. W niniejszej pracy przeanalizowano różne techniki znakowania wodnego, obejmujące zarówno tradycyjne algorytmy, jak i nowoczesne systemy oparte na głębokich sieciach neuronowych. Celem badań było porównanie odporności tych metod na różne aktualnie występujące ataki w mediach społecznościowych. Do eksperymentów wykorzystano rozbudowany zbiór danych zawierający zdjęcia o zróżnicowanych parametrach. Na każdy obraz został nałożony znak wodny, który w następnych etapach był atakowany. Największy wpływ na ekstrakcję znaku wodnego miały ataki takie jak kompresja stratna JPEG, rozmycie obrazu oraz dodanie szumu. Po każdym kroku były zbierane metryki takie jak BER, QualiCLIP, LPIPS, SSIM, na podstawie których oceniano skuteczność algorytmów. Eksperymenty wykazały, że ataki bazujące na kompresji stratnej oraz rozmywaniu obrazu miały największy wpływ na ekstrakcję znaku wodnego, utrudniając odzyskanie osadzonych znaków w przeciwieństwie do ataków opartych na szumie, które miały niewielki wpływ. Metoda naiwna, wykorzystująca obraz źródłowy przy dekodowaniu, wykazuje najlepszą przeżywalność ataków. Metody oparte na głębokich sieciach neuronowych również okazały się skuteczne, jednak ich czas działania był znacząco dłuższy.

Authors: PILEWSKI, Adam; Dr HRYNIÓW, Krzysztof (Warsaw University of Technology); KORDOWSKI, Mikołaj

Presenters: PILEWSKI, Adam; KORDOWSKI, Mikołaj

Session Classification: Session C (Poster)

Contribution ID: **34** Type: **Poster**

Comparison of Models for Automatic Description of Medical Images

Thursday 24 April 2025 10:45 (30 minutes)

Automated medical report generation from chest X-ray images is a critical area of research in medical AI, aiming to enhance diagnostic accuracy, reduce radiologists' workload, and improve patient care. The process involves analyzing medical images and translating visual findings into structured, clinically relevant textual reports. Traditional methods rely on human expertise, which is time-consuming and prone to variability, motivating the development of deep learning-based solutions that leverage vision-language models to automate this task. This project explores and compares state-of-the-art deep learning architectures for medical report generation, evaluating their capabilities in image encoding and text generation. The study considers convolutional neural networks (CNNs) such as ResNet, vision transformers (ViTs) like SwinTransformer, and state space models (SSMs) such as Mamba for extracting visual features. The text generation stage utilizes recurrent neural networks (RNNs) such as LSTMs and GRUs, as well as transformer-based architectures such as BioClinicalBERT, LLaMA-2, and GPT-style decoders. The models being evaluated include BioViL-T, R2Gen, MedCLIP, PLIP, CheXbert, and MambaXray-VL, trained and tested on datasets such as IU X-Ray and CheXpert. This study aims to systematically assess different architectural approaches, training methodologies, and dataset utilization strategies to provide insights into their advantages and limitations in generating clinically meaningful radiology reports.

Author: Mr URBAŃSKI, Jakub (Warsaw University of Technology)

Presenter: Mr URBAŃSKI, Jakub (Warsaw University of Technology)

Session Classification: Session B (Poster)

Contribution ID: **35** Type: **Poster**

Zastosowanie modeli GAN do usuwania artefaktów z sygnału EEG

Thursday 24 April 2025 10:45 (30 minutes)

Sygnał elektroencefalograficzny (EEG) może ulegać zakłóceniom spowodowanym przez aktywność elektryczną niezwiązaną bezpośrednio z pracą mózgu badanego. Zjawisko to określane jest jako problem artefaktów EEG, które dzielimy na techniczne i fizjologiczne. Do artefaktów fizjologicznych należą charakterystyczne fragmenty sygnału rejestrowane w wyniku ruchów gałek ocznych, mrugania, czy aktywności mięśniowej. W celu eliminacji tych zakłóceń opracowano wiele metod, spośród których najczęściej stosowane to ślepa separacja sygnałów, empiryczna dekompozycja modalna oraz transformata falkowa. Kluczowym wyzwaniem jest minimalizacja utraty istotnych informacji podczas usuwania artefaktów. W ostatnich latach coraz większą popularność zyskują metody wykorzystujące uczenie maszynowe. Szczególnie obiecujące wyniki uzyskano dzięki zastosowaniu sieci konwolucyjnych, autoenkoderów oraz sieci GAN. Techniki te mają potencjał adaptowania się do eliminacji artefaktów o różnorodnej charakterystyce. W artykule przedstawiono wyniki zastosowania sieci GAN wraz z dodatkowymi sygnałami artefaktu w celu eliminacji artefaktów fizjologicznych. Modele były trenowane na danych syntetycznych zawierających artefakty typu EOG oraz EMG. Uzyskane wyniki sugerują, że zastosowanie sieci GAN w połączeniu z sygnałami EMG może skutecznie wspomóc usuwanie artefaktów fizjologicznych z zapisu EEG.

Author: SOKÓŁ, Małgorzata (Wydział Elektryczny, Politechnika Warszawska)

Co-author: Dr KOŁODZIEJ, Marcin (Instytut Elektrotechniki Teoretycznej i Systemów Informacyjno-Pomiarowych, Wydział Elektryczny, Politechnika Warszawska)

Presenter: SOKÓŁ, Małgorzata (Wydział Elektryczny, Politechnika Warszawska)

Session Classification: Session B (Poster)

Contribution ID: **36** Type: **Poster**

Blazor WebAssembly and React comparison

Thursday 24 April 2025 11:30 (30 minutes)

The choice of a frontend framework significantly impacts the performance, maintainability, and scalability of modern web applications. This paper presents a comparative analysis of Blazor and React, two popular frontend frameworks with distinct architectures and approaches to building web interfaces. Blazor, developed by Microsoft, leverages C# and .NET to enable web development using WebAssembly or server-side rendering. React, maintained by Meta, is a widely adopted JavaScript library that utilizes a virtual DOM and component-based architecture.

This study compares the performance of React and Blazor by replicating a set of benchmarks focused on measuring rendering efficiency. The benchmarks analyze three key scenarios: rendering static elements, rendering a large number of child components, and constructing a binary tree component hierarchy. By measuring the time required for each rendering operation, this research provides insights into the performance characteristics of these frameworks, highlighting their strengths and weaknesses in different rendering scenarios.

Author: OLSZEWSKI, Antoni (Politechnika Warszawska, Wydział Elektryczny)

Presenter: OLSZEWSKI, Antoni (Politechnika Warszawska, Wydział Elektryczny)

Session Classification: Session C (Poster)

Contribution ID: **37** Type: **Poster**

Machine Learning-Based Examination of ESG Factors in Stock Predictions

Thursday 24 April 2025 11:30 (30 minutes)

This paper explores the relationship between carbon reduction efforts, ESG factors and financial performance. Machine learning models are applied to multi-industry data to assess whether carbon-related ESG attributes - such as carbon emissions and participation in emissions trading schemes - enhance the prediction of stock returns. The analysis also considers the concept of a carbon premium, understood as the excess return investors may require from firms with high greenhouse gas emissions. The findings indicate that, although such ESG indicators are widely disclosed, their inclusion does not consistently improve model accuracy and, in some cases, diminishes predictive performance due to data gaps and increased complexity. The results suggest that ESG-related factors, particularly those linked to carbon emissions, may not directly or immediately influence a firm's financial returns, underscoring the need for more comprehensive data to evaluate their long-term significance.

Authors: STAŃKOWSKI, Daniel (Warsaw University of Technology); Mr ŚLUSARCZYK, Daniel (Warsaw University of Technology); Mr TĘCZA, Paweł (Warsaw University of Technology)

Presenters: STAŃKOWSKI, Daniel (Warsaw University of Technology); Mr ŚLUSARCZYK, Daniel (Warsaw University of Technology); Mr TĘCZA, Paweł (Warsaw University of Technology)

Session Classification: Session C (Poster)

Contribution ID: **38** Type: **Presentation**

Optimization of neural network model for malware detection accelerated on mobile NPUs

Thursday 24 April 2025 10:16 (12 minutes)

With the increasing number of cyber threats, malware detection has become a critical challenge in cybersecurity. Traditional detection techniques, based on behavioral analysis and signature creation, present significant challenges due to their time-consuming nature and limited effectiveness against new, unknown threats. This paper explores the optimization of artificial intelligence (AI) for malware detection, leveraging acceleration on mobile neural processing units (NPUs). The primary goal of this study is to develop and evaluate methods that enhance machine learning models in terms of computational efficiency and detection accuracy in resource-constrained environments.

The research methodology involved designing the initial model on a high-performance computing system to determine the optimal network size that balances processing speed and detection precision across various devices. A more precise version of the model was subsequently trained on more powerful hardware, followed by the application of optimization techniques to adapt it for execution on mobile NPUs.

The study examines the performance of different NPU architectures and assesses the impact of operating systems on the efficiency and speed of AI-based detection models. Preliminary findings indicate that the applied optimizations have led to satisfactory results in detecting malicious code within binary files on Windows systems.

This research contributes to the development of AI deployment methods on mobile devices, which can significantly enhance end-user security without relying on external cloud-based solutions. Future studies aim to expand the analysis to software running on other platforms.

Author: Mr KONARSKI, Jan

Presenter: Mr KONARSKI, Jan

Session Classification: Session A (Presentation)

Contribution ID: **39** Type: **Poster**

Exploring LLMs mathematical reasoning capability: Insights from GSM-Symbolic in English and Polish

Thursday 24 April 2025 10:45 (30 minutes)

Large language models (LLMs) are trained with ever-increasing amounts of data. It seems that when asked to solve mathematical tasks, they can infer and reason mathematically [1]. The GSM8K benchmark platform is widely used to test various LLMs to solve simple arithmetic tasks. Recently, LLMs have shown a clear improvement in their ability to correctly answer questions from the GSM8K dataset. However, it is impossible to say conclusively from the GSM8K studies whether the performance increase was also followed by improvements, in the mathematical reasoning mentioned above. A recent study that shed light on the problem of mathematical reasoning in LLMs [2] attempted to address this problem by creating a database based on GSM8K but with the ability to make appropriate changes to the content of math tasks, which would test how true the claim that LLMs can reason is.

In our research, we have attempted to confirm previously established research results, but also to extend them to include newly developed language models such as DeepSeek or more advanced versions of ChatGPT. Above that, the research was also extended to check the influence of the language in which the test math tasks were written on the effectiveness of a given model. We decided to translate the GSM-Symbolic datasets using the Google Translator API, creating Polish equivalents, which we have provisionally named GSM-Symbolic-PL, GSM-P1-PL, GSM-P2-PL. The selected LLMs are then questioned hundreds of times using the 3-shot Chain-of-Thought prompting method [3], which involves giving the model 3 sample questions and answers to indicate how the model should ”think”when generating and answer to the final question. Using it is supposed to allow LLMs to be more directed towards proper mathematical thinking and reasoning which we want to investigate. After that, the results were validated and analyzed.

Our research was focused on ChatGPT versions 4o-mini and o3-mini and DeepSeek's latest versions V3 and R1. As expected, the model's responses depend on the content of the task and is strongly dependent on whether bias is placed in the task, in which case the model makes errors very often. This seems to indicate that LLMs might not be able to reason mathematically the way humans do. Their answers are inconsistent, even though the reasoning path to solve the task remains the same. GSMSymbolic, compared to GSM8K, exposed this weakness even more, but this does not change the fact that the higher models'correctness of response is quite high.

Authors: ŁOMIŃSKI, Marcin (Wydział Elektryczny, Politechnika Warszawska); TOMCZYK, Michał (Wydział Elektryczny, Politechnika Warszawska)

Presenters: ŁOMIŃSKI, Marcin (Wydział Elektryczny, Politechnika Warszawska); TOMCZYK, Michał (Wydział Elektryczny, Politechnika Warszawska)

Session Classification: Session B (Poster)

Contribution ID: **40** Type: **Poster**

Franky: An Intelligent Agent for Stock Portfolio Management Using Large Language Models and Deep Reinforcement Learning

Thursday 24 April 2025 10:45 (30 minutes)

Franky: An Intelligent Agent for Stock Portfolio
Management Using Large Language Models and
Deep Reinforcement Learning

1st Mikołaj Zawada*
Faculty of Electrical Engineering
Warsaw University of Technology
Warsaw, Poland
mikolaj.zawada.stud@pw.edu.pl
2nd Mateusz Bartosik*
Faculty of Electrical Engineering
Warsaw University of Technology
Warsaw, Poland
mateusz.bartosik.stud@pw.edu.pl
3rd ˙Zaneta ´Swiderska-Chadaj, PhD†
Faculty of Electrical Engineering
Warsaw University of Technology
Warsaw, Poland
zaneta.swiderska@pw.edu.pl

I. INTRODUCTION

This paper introduces an innovative intelligent trading agent designed for autonomous stock portfolio management, integrating Large Language Models (LLMs) and Deep Reinforcement Learning (DRL). The core objective was to develop a trading agent capable of effectively managing a diversified stock portfolio by synthesizing quantitative market data with qualitative insights derived from real-time financial news and corporate reports.

The motivation behind this approach arises from limitations observed in conventional trading algorithms, which predominantly rely on historical price data and technical indicators while frequently neglecting critical qualitative information. Existing market solutions typically separate numerical analysis and text-driven sentiment analysis, thus failing to fully exploit the synergistic potential of these data sources. By contrast, the proposed method uniquely integrates these elements through a combined architecture inspired by FINMEM [1] and FinRL [2] frameworks.

The proposed system operates through a multi-layered approach, employing DRL agents trained on historical numerical data and stock-specific memory module that prioritize and manage textual information. Memory module continuously captures, processes, and contextualizes incoming data streams into structured, actionable insights. Data is being scraped and processed in real-time from predefined and trusted sources on the Internet, allowing a rapid reaction to ever changing market environment. LLM serve as an advanced interpretative engine, conducting sentiment and contextual analyses of news articles to anticipate market reactions. DRL Agent is responsible for a quantitative analysis of portfolio assets and suggesting an optimized resources allocation. It considers how assets move relative to each other, risks associated with each asset, technical indicators and historical data. Agent is using the Advantage Actor-Critic [3] algorithm that, after a series of backtesting, outperformed DDPG, PPO, TD3 and SAC [4] by around 5%-20%. Ultimately, stock-level recommendations are integrated by a dedicated portfolio-level LLM, considering portfolio constraints, diversification, risk tolerance, and available funds to formulate cohesive and strategic trading decisions. As many LLMs of various architectures are currently available, such a selection of them was taken into consideration which enabled verification of the difference between reasoning and non-reasoning models.

Validation of the system's performance was conducted through rigorous backtesting across diverse historical market conditions, employing metrics such as cumulative returns and risk-adjusted returns against benchmark trading strategies. Initial results (return of around 36%) demonstrate the superior performance and adaptability of the proposed system, outperforming conventional DRL-based and purely sentiment-based methods, particularly in volatile market conditions.

Future development will concentrate on optimizing the portfolio manager component, exploring dynamic rebalancing strategies and refining its scalability and adaptability to real-time trading environments. This work not only enhances autonomous trading technologies but also provides valuable insights into how hybrid AI architectures can revolutionize financial market analysis and decision-making.

Index Terms—Large Language Models, Deep Reinforcement Learning, Stock Trading, Portfolio Management

* Equal contribution

† Supervisor

REFERENCES

[1] Y. Yu, H. Li, Z. Chen, Y. Jiang, Y. Li, D. Zhang, R. Liu, J. W. Suchow, and K. Khashanah, "Finmem: A performance-enhanced llm trading agent with layered memory and character design,"2023. [Online]. Available: https://arxiv.org/abs/2311.13743

[2] X.-Y. Liu, H. Yang, Q. Chen, R. Zhang, L. Yang, B. Xiao, and C. D. Wang, "Finrl: A deep reinforcement learning library for automated stock trading in quantitative finance,"2022. [Online]. Available: https://arxiv.org/abs/2011.09607

[3] G. Song, T. Zhao, X. Ma, P. Lin, and C. Cui, "Reinforcement learning-based portfolio optimization with deterministic state transition,"Information Sciences, vol. 690, p. 121538, 2025.
[4] S. Liu, "An evaluation of ddpg, td3, sac, and ppo: Deep reinforcement learning algorithms for controlling continuous system,"in Proceedings of the 2023 International Conference on Data Science, Advanced Algorithm and Intelligent Computing (DAI 2023). Atlantis Press, 2024, pp. 15–24. [Online]. Available: https://doi.org/10.2991/978-94-6463-370-23

Authors: BARTOSIK, Mateusz (Warsaw University of Technology); ZAWADA, Mikolaj (Warsaw University of Technology)

Co-author: Dr ŚWIDERSKA-CHADAJ, Żaneta (Warsaw University of Technology)

Presenters: BARTOSIK, Mateusz (Warsaw University of Technology); ZAWADA, Mikolaj (Warsaw University of Technology)

Session Classification: Session B (Poster)

Contribution ID: **41** Type: **Poster**

Automatic translation of Japanese manga using MultiModal Large Language Models

Thursday 24 April 2025 10:45 (30 minutes)

Japanese manga has captivated readers worldwide with its vibrant and expressive form of art that provides compelling storytelling with intricate visuals. However, for many fans outside of Japan, language barriers often stand in the way of fully experiencing the depth of these stories. Traditional translation from language to language, while effective, can be a very time-consuming and labor-intensive process that requires teams of translators, editors, and cultural consultants to convey the essence of the original text accurately. The difficulty with Japanese is even greater, as it is a heavy-context-intensive language.

Machine translation is nothing new; we try and fail with basic translation from language A to language B, and Google Translate is its finest example. Large language models (LLMs) and with its new type, multimodal LLMs, have undergone substantial advancements, augmenting already powerful LLMs to support multimodal inputs or outputs via cost-effective training strategies. Those showed potential in many works such as coding, answering complex math questions, or understanding symbolism within texts. In this paper, we conduct a substential investigation on how well certain MMLLMs work against manga translation. We create benchmarks with text-only-wise; image-from1page-context; as well as whole volume thus far.

Although the results were sometimes satisfactory, they proved to be insufficient to be a standalone automatic translator, as translations were not understandable and/or too complex or too simple at times. However they prove to provide enough understanding of context to, with some human element, come up with accurate translation

Author: NITSCH, Tomasz (Warsaw University of Technology)

Presenter: NITSCH, Tomasz (Warsaw University of Technology)

Session Classification: Session B (Poster)

Contribution ID: **42** Type: **Poster**

Proxy Methods in Image Recognition

Thursday 24 April 2025 10:45 (30 minutes)

This paper presents a comprehensive comparison of several state-of-the-art proxy loss methods for retail product recognition, focusing on accuracy, computational efficiency, embedding quality, and convergence behaviour. An extensive evaluation is performed on the Stanford Online Products benchmark dataset, which contains over 120,000 images covering 22,634 distinct product categories. The analysis reveals a trade-off between proxy-based and non-proxy-based methods, highlighting the conditions under which each approach may be more advantageous. Attention is also given to identifying optimal model parameters for individual proxy methods, offering insights into their most effective configurations. The findings underscore the importance of balancing computational efficiency and embedding quality when deploying proxy loss methods for large-scale product recognition tasks.

Authors: BORKOWSKA, Barbara; MACIĄG, Marcin

Presenters: BORKOWSKA, Barbara; MACIĄG, Marcin

Session Classification: Session B (Poster)

Contribution ID: **43** Type: **Poster**

Threat Detection in IIoT Networks through Deep Packet Inspection and Machine Learning Mechanisms

Thursday 24 April 2025 11:30 (30 minutes)

The rapid expansion of Industrial Internet of Things (IoT) networks has increased security vulnerabilities, necessitating robust threat detection mechanisms. Industrial networks may hold non-critical data and confidential energy or medical data. The second group should therefore be covered by stringent security policies against Denial of Service attacks or attempts to steal information through an unsecured network segment. The traditional approach to analyzing network traffic is to classify packets as suspicious based only on the initial layers of the TCP/IP model; such a solution is sufficient for security policies designed to ensure business continuity of systems, but rejects the possibility of advanced detection based on application layer protocols investigation. Therefore, modern threat detection solutions have security capabilities extended with the DPI (Deep Packet Inspection) technique, using application layer data analysis for security improvement.

This research investigates the effectiveness of deep packet inspection (DPI) and machine learning (ML) techniques in detecting cyber threats across protocols like MQTT, SNMP, and Modbus. Using the pipeline consisting of the packet capture samples preprocessor and pre-trained binary classification model, we extract packet-level features and analyze protocol-specific anomalies, classifying the network traffic sample as malicious or normal activity. The study compares the performance of Random Forest, Naive Bayes, and a Neural Network. The Random Forest model, configured with 100 trees and a maximum depth of 5, demonstrates strong predictive capabilities. Naive Bayes leverages probabilistic classification, while the Neural Network, structured with two hidden layers and trained using the Adam optimizer, effectively captures complex traffic patterns. The study employs three classification models: Random Forest, Naive Bayes, and a Neural Network. The Random Forest classifier is configured with 100 trees and a maximum depth of 5. The Naive Bayes model utilizes Gaussian probability distributions for classification. The Neural Network consists of a multi-layer perceptron with two hidden layers of 40 and 20 neurons, using ReLU activation functions and trained with the Adam optimizer. Experimental results demonstrate the model's capability to identify protocol-specific threats with high accuracy, showcasing the potential of DPI-driven ML approaches for securing IIoT environments.

Author: GUZIUK, Jan

Co-author: MASŁOWSKI, Hubert (Warsaw University of Technology)

Presenter: MASŁOWSKI, Hubert (Warsaw University of Technology)

Session Classification: Session C (Poster)

Contribution ID: **44** Type: **Poster**

Selected methods in N-body simulations

Thursday 24 April 2025 11:30 (30 minutes)

This paper discusses the implementation of the particle-mesh (PM) and particle-particle particle-mesh (P3M) methods in the context of a spiral galaxy simulation. Simulations performed using both methods correctly predict the formation of characteristic spiral arms and demonstrate expected physical behavior, satisfying Newton's second law and conserving energy and angular momentum. The PM code was written for both the CPU and GPU architectures, with the GPU version achieving approximately sevenfold speedup compared to the multithreaded CPU implementation.

Author: BAŁAZIŃSKI, Aleksy (Warsaw University of Technology)

Presenter: BAŁAZIŃSKI, Aleksy (Warsaw University of Technology)

Session Classification: Session C (Poster)

Contribution ID: **45** Type: **Poster**

Optimizing Football Betting Strategies Using Deep Neural Networks and Modern Portfolio Theory

Thursday 24 April 2025 10:45 (30 minutes)

This paper presents a hybrid framework combining Deep Neural Networks (DNNs) and Modern Portfolio Theory (MPT) to optimize football betting strategies. Leveraging historical match data from five major European leagues (2014–2025), we engineer predictive features such as dynamic Elo rankings, expected goals (xG), and team performance metrics derived from raw game statistics. Diverse neural architectures, including convolutional (Conv1D) and recurrent (LSTM, GRU) layers, are systematically explored to capture spatial and temporal patterns in match outcomes and goal totals. Automated Machine Learning (AutoML) techniques further refine model selection and hyperparameter tuning, ensuring robustness. MPT principles are then applied to balance risk and return, evaluating strategies ranging from threshold-based betting to a modified Kelly Criterion. The synergy of advanced predictive modeling, automated architecture optimization, and systematic risk management provides a scalable, data-driven pathway to sustainable profitability in sports betting.

Authors: KUCIŃSKI, Daniel; Mr MYCIELSKI, Tomasz (Warsaw University of Technology)

Presenters: KUCIŃSKI, Daniel; Mr MYCIELSKI, Tomasz (Warsaw University of Technology)

Session Classification: Session B (Poster)

Contribution ID: **46** Type: **Poster**

Performance Comparison of WebAssembly and JavaScript

Thursday 24 April 2025 11:30 (30 minutes)

JavaScript remains the dominant language for client-side scripting, while WebAssembly offers near-native execution speeds, making it a compelling choice for computationally intensive tasks. This study provides a comprehensive analysis of the performance differences between WebAssembly and JavaScript across various computing environments, including different browsers (Firefox, Chrome, Edge) and platforms (desktop and mobile) [1], [2].

To evaluate computational efficiency, we conducted a series of benchmark tests, including integer operations (Sieve of Eratosthenes, sorting algorithms) [3], floating-point calculations (numerical integration, Monte Carlo method) [4], and recursive computations (Fibonacci sequence, matrix multiplication) [5]. Additionally, we investigated the impact of WebAssembly on machine learning workloads by utilizing minimalist implementations such as TinyDNN for digit classification on the MNIST dataset [6]. Our findings indicate that WebAssembly consistently outperforms JavaScript in CPU-bound tasks, particularly in integer operations and recursive computations. However, JavaScript's just-in-time (JIT) compilation allows it to remain competitive in some floating-point calculations.

One focus of our study was the application of WebAssembly in browser-based machine learning. We examined the performance of lightweight neural network implementations, emphasizing WebAssembly's ability to accelerate tensor computations directly in the browser. This capability is crucial for deploying AI models on the client side, reducing reliance on cloud-based services, improving privacy, and minimizing latency. Our analysis also explores WebAssembly's potential for real-time applications such as image classification, object detection, and natural language processing.

Beyond raw performance metrics, this study assesses the broader implications of WebAssembly's adoption in web development. One of its key advantages is its ability to support multiple programming languages, including Rust, C, and C++, allowing developers to leverage high-performance libraries within the browser environment [7]. Additionally, WebAssembly's sandboxing mechanisms enhance security by isolating execution, reducing potential attack vectors compared to traditional JavaScript-based applications.

Despite its advantages, WebAssembly has limitations. Exe

cution performance varies across browsers, and its integration with JavaScript-based applications presents challenges due to data serialization overhead. Moreover, WebAssembly lacks direct access to the DOM, necessitating JavaScript as an intermediary for UI interactions.

As WebAssembly continues to evolve, its role in performance critical web applications is expected to expand, particularly in fields such as cryptography, data processing, and real-time machine learning.

Keywords—WebAssembly, JavaScript, Performance Compar ison, Machine Learning, Convolutional Neural Networks.

Authors: CISZEWSKI, Jakub (PW EE); MYK, Kaja

Presenters: CISZEWSKI, Jakub (PW EE); MYK, Kaja

Session Classification: Session C (Poster)

Contribution ID: **47** Type: **Poster**

Testy penetracyjne systemu zarządzania energią elektryczną OpenEMS —identyfikacja i mitygacja podatności w otwartoźródłowych systemach energetycznych

Thursday 24 April 2025 10:45 (30 minutes)

W odpowiedzi na rosnącą popularność rozproszonych systemów zarządzania energią oraz integrację odnawialnych źródeł energii (OZE), w projekcie przeprowadzono kompleksową analizę bezpieczeństwa otwartoźródłowego systemu OpenEMS. System ten, napisany w języku Java, wspiera monitorowanie, kontrolę i optymalizację przepływów energii elektrycznej w instalacjach przemysłowych i prosumenckich. Celem projektu była identyfikacja krytycznych podatności w systemie oraz ocena ryzyka dla integralności, dostępności i poufności danych w kontekście systemów zarządzających infrastrukturą energetyczną. Zidentyfikowano problematykę związaną z brakiem powszechnie dostępnych analiz bezpieczeństwa otwartoźródłowych systemów EMS, mimo ich rosnącego znaczenia w przemyśle i energetyce. W trakcie badań przeprowadzono testy penetracyjne obejmujące, analizę kodu źródłowego i komponentów backendu, testy dynamiczne interfejsów REST API, ocenę bezpieczeństwa warstwy komunikacji Modbus TCP, badanie podatności na typowe błędy programistyczne i konfiguracyjne. Do realizacji testów wykorzystano m.in. środowiska OWASP ZAP, Burp Suite, a także specjalistyczne narzędzia dedykowane testowaniu systemów OT i aplikacji webowych. Przeanalizowano krytyczne błędy w kodzie źródłowym oraz zaproponowano zmiany w konfiguracji komunikacji sieciowej, zwiększające odporność systemu na ataki. Projekt dostarczył istotnych wniosków naukowych, pogłębiając wiedzę z zakresu cyberbezpieczeństwa otwartoźródłowych systemów klasy EMS. Wyniki badań wykazały powtarzalne wzorce podatności charakterystyczne dla tego typu rozwiązań i potwierdziły konieczność łączenia podejścia IT z praktykami ochrony infrastruktury krytycznej (OT). Z perspektywy praktycznej i komercyjnej projekt przyniósł mierzalną wartość dla podmiotów wdrażających OpenEMS w rzeczywistych instalacjach przemysłowych i prosumenckich. Opracowane rekomendacje mogą zostać bezpośrednio wykorzystane w audytach bezpieczeństwa oraz jako podstawa dla dalszego rozwoju systemu, zwiększając jego odporność na zagrożenia cybernetyczne.

Author: GORLOWSKI, Kacper

Presenter: GORLOWSKI, Kacper

Session Classification: Session B (Poster)

Contribution ID: **48** Type: **Poster**

Enhancing Large Language Models with Retrieval-Augmented Generation: A Case Study on Movie Data Beyond the Training Cutoff

Thursday 24 April 2025 10:45 (30 minutes)

This article investigates the role of Retrieval-Augmented Generation (RAG) in enhancing Large Language Models (LLMs) with information about movies and TV series released beyond their training data. In this study, the Llama 3.2 3B LLM is leveraged and integrated with external movie-related data retrieved from the OMDb API to provide specific information about over 14000 titles released in 2024, which fall outside of the LLM's knowledge cutoff. This approach aims to improve the accuracy, reliability, and contextual relevance of LLM responses by utilizing movie metadata and precomputed embeddings for information retrieval. The incorporation of these techniques enables the system to efficiently identify plot connections, verify directors and cast members, and analyze trends in the latest movie productions. Moreover, the research examines RAG's potential in mitigating LLM hallucinations by providing reliable external knowledge and adaptive query processing. The results aim to support film critics, analysts, and movie enthusiasts by providing the latest film-related data, while also highlighting the effectiveness of RAG in fields where access to specialized, dynamic knowledge is crucial.

Author: MIKOŁAJCZYK, Marcel (Politechnika Warszawska, Wydział Elektryczny)

Presenter: MIKOŁAJCZYK, Marcel (Politechnika Warszawska, Wydział Elektryczny)

Session Classification: Session B (Poster)

Contribution ID: **49** Type: **Poster**

Wpływ facylitacji na efektywność spotkań w projektach IT

Thursday 24 April 2025 11:30 (30 minutes)

Efektywna komunikacja między zespołami IT a biznesem jest jednym z kluczowych czynników sukcesu projektów. Jednak różnice w oczekiwaniach, niejasne wymagania oraz nieskuteczne spotkania często prowadzą do barier we współpracy. Niniejsza praca identyfikuje najistotniejsze wyzwania komunikacyjne oraz analizuje wpływ technik facylitacyjnych na usprawnienie współpracy w projektach IT, koncentrując się na studium przypadku startupu tworzącego mobilną grę do nauki języków. Badania obejmują ocenę, w jaki sposób strukturalne metody facylitacyjne wpływają na budowanie porozumienia między członkami zespołu projektowego. Analizowany przypadek przedstawia ewolucję uczestników, którzy w miarę wzrostu napotykali trudności komunikacyjne i sukcesywnie je eliminowali dzięki zastosowaniu facylitacji. Zdefiniowano główne bariery komunikacyjne, jak różnice priorytetów, brak jasności, pomijanie wypowiedzi i niedostateczne zaangażowanie. Najbardziej przydatnym metodami facylitacyjnymi okazały się Poza zakresem, Diagram Przepływu, Parafrazowanie oraz Agenda procesu. Otrzymane wyniki sugerują, że facylitacja jest wartościowym narzędziem w projektach IT, które może wspierać zespoły w skutecznym rozwiązywaniu konfliktów, budowaniu atmosfery współpracy i zwiększeniu produktywności spotkań.

Author: Ms VASILCHYK, Darya (Politechnika Warszawska)

Presenter: Ms VASILCHYK, Darya (Politechnika Warszawska)

Session Classification: Session C (Poster)

Contribution ID: **50** Type: **Poster**

Ethereum price forecasting using deep neural networks

Thursday 24 April 2025 10:45 (30 minutes)

Short-term forecasting of cryptocurrency prices remains a challenging task due to the high volatility and complex market dynamics of digital assets like Ethereum. This study proposes a hybrid deep learning model, that integrates networks such as Bi-LSTM, FinBERT and GRU, seeking to provide a comprehensive analysis of their applicability in this domain and enhance predictive accuracy for this currency. It incorporates news sentiment analysis as an additional predictive feature, aiming to capture broader market sentiment trends. The model was trained using historical Ethereum price data, along with trading volume, technical indicators, and sentiment scores extracted from news sources. Results indicate that the hybrid model outperforms traditional standalone models, suggesting that combining multiple architectures improves short-term price forecasting. However, challenges such as sentiment data noise and potential overfitting highlight areas for further refinement.

Author: ROZWADOWSKI, Oskar (Warsaw University of Technology)

Presenter: ROZWADOWSKI, Oskar (Warsaw University of Technology)

Session Classification: Session B (Poster)

Contribution ID: **51** Type: **Poster**

Pose-Based Motion Analysis for Physical Exercise Quality Assessment

Thursday 24 April 2025 10:45 (30 minutes)

This paper presents a comprehensive approach to the evaluation of physical exercise using skeletal estimation and motion analysis. The research begins with the acquisition of relevant datasets and a review of existing monocular pose estimation solutions. A key component of this work is modeling important features, including skeletal joint weighting and key angles between them, according to their relevance for specific exercises. The synchronization of reference and analyzed recordings is achieved using Dynamic Time Warping (DTW), enabling accurate comparison and alignment.

We propose a method to determine the correct measure of consistency between reference and estimated trajectories, along with setting DTW distance thresholds based on performance quality. Finally, the effectiveness of the developed solution is assessed, and strategies for its optimization are discussed. The proposed approach offers valuable insights into improving motion estimation accuracy for exercise monitoring and analysis.

Author: JAKIEŁA, Wojciech (Politechnika Warszawska)

Co-author: Dr CHABER, Bartosz (Politechnika Warszawska)

Presenter: JAKIEŁA, Wojciech (Politechnika Warszawska)

Session Classification: Session B (Poster)

Contribution ID: **52** Type: **Poster**

Low-cost, home-made Quantum Computer

Thursday 24 April 2025 11:30 (30 minutes)

This presentation explores the development of a low-cost, home-built quantum computer aimed at validating hypotheses from numerical simulations, combining theoretical advancements in quantum computing with practical engineering solutions. Three configurations are discussed: an Intel Labs-inspired setup demonstrating pulse-level control programming with PennyLane and benchmarking using the Deutsch-Jozsa algorithm; a detailed guide to implementing the Deutsch-Jozsa algorithm at home, supported by foundational quantum information science principles; an approach to generating entanglement through nonlinear effects in Beta Barium Borate (BBO) crystals, leveraging Kerr effects. The project underscores the feasibility of constructing functional quantum systems outside specialized laboratories, and highlights the potential for democratizing access to quantum technologies.

Author: KOŁCZ, Hubert (Warsaw University of Technology)

Co-authors: Mr ŁABAJ, Filip (Warsaw University of Technology); Ms PRZYBYŁA, Gabriela (Warsaw University of Technology); Mr RUKAT, Paweł (Warsaw University of Technology); Mr MARUSZAK, Piotr (Warsaw University of Technology)

Presenter: KOŁCZ, Hubert (Warsaw University of Technology)

Session Classification: Session C (Poster)

Contribution ID: **53** Type: **Poster**

Database Index Costs in the Cloud-Based Multitenant Architecture on the Salesforce Platform

Thursday 24 April 2025 11:30 (30 minutes)

Study on how in the multitenant cloud architecture of the Salesforce platform, different field configurations available to administrators impact database index usage, query costs, and data manipulation language operations. Results show that while “External ID” and “Unique” settings consistently create indexes with varying performance effects, the “Required” flag unexpectedly affects query costs in a meaningful manner. Results highlight the need for case-by-case tuning using the Salesforce Query Planner.

database indexes, Salesforce, multi-tenant architecture, database tuning, CRM

Author: ZAŃ, Stanislaw (Polish-Japanese Academy of Information Technology)

Presenter: ZAŃ, Stanislaw (Polish-Japanese Academy of Information Technology)

Session Classification: Session C (Poster)

Contribution ID: **54** Type: **Presentation**

Line Follower Algorithm for a Flying Quadcopter

Thursday 24 April 2025 10:06 (10 minutes)

Line Follower Algorithm for a Flying Quadcopter

Mikołaj Stasiak, Wiktor Ważny, Grzegorz Zając

Institute for Automation and Robotics, Faculty of Mechatronics, Warsaw University of Technology.

As interest in aerial drones and autonomous systems grows, so does the need for optimal solutions that can be run on minimalistic hardware. This paper describes an autonomous, vision-based algorithm designed for participation in the MathWorks Minidrone Competition. The algorithm was developed within competition's specification [1] and the authors won the 3rd place in the nationwide MathWorks Minidrone Competition Poland 2025 [2]. The work done included research on publicly available, already existing solutions [3] as well as on tools that could be applied to the task at hand [4], [5]. As a result a custom vision algorithm was developed to balance fidelity and speed and to minimise the computing power required. The drone software, written entirely in Matlab is capable of controlling a Parrot Mambo mini drone tasked with traversing a course made of red straight lines joined at different angles. The programme is designed around a built-in low-resolution camera pointing downwards. The work focuses on the design and development of an image processing algorithm as well as path planner and flight control programs that transform a low resolution image into a list of instructions for the drone.

Full version with pictures can be found attached below.

References
[1] Contest rules: https://www.mathworks.com/content/dam/mathworks/mathworks-dot-com/academia/student-competitions/minidrone-competition/mathworks-minidrone-competition-guidelines.pdf
[2] Contest results: https://ont.com.pl/wydarzenia/minidrone-poland-25
[3] Projects reviewed: https://github.com/Rutwik1000/Parrot-Minidrone-Competition/tree/f176186176548ac9ab66335d6225048e436e043c; https://github.com/mar4945/Vision-Based-Pure-Pursuing-Algorithm
[4] Min-max algorithm: https://arxiv.org/abs/2011.14035
[5] Imfindcircles function: https://www.mathworks.com/help/images/ref/imfindcircles.html

Authors: Mr ZAJĄC, Grzegorz (Warsaw University of Technology (PL)); STASIAK, Mikolaj (Warsaw University of Technology (PL)); Mr WAŻNY, Wiktor (Warsaw University of Technology (PL))

Presenter: STASIAK, Mikolaj (Warsaw University of Technology (PL))

Session Classification: Session A (Presentation)

Contribution ID: **55** Type: **Poster**

A Survey of Consensus Algorithms in Distributed Ledger Technology for Internet of Things

Thursday 24 April 2025 11:30 (30 minutes)

This comprehensive survey examines consensus algorithms utilized in Distributed Ledger Technology (DLT) for Internet of Things (IoT) environments. The paper provides a comparative analysis of consensus protocols including Proof of Work, Proof of Stake, Proof of Authority, Proof of Elapsed Time, Proof of Space, Proof of Activity, Practical Byzantine Fault Tolerance algorithm and Directed Acyclic Graph based approaches such as Adaptive Proof of Work, and Temporal Proof. These algorithms are evaluated against critical metrics for IoT contexts: energy efficiency, transaction throughput, scalability, latency, and security guarantees. The survey highlights fundamental trade-offs between decentralization, security, and performance in DLT implementations, with particular focus on mechanisms compatible with resource-constrained IoT networks. Through this systematic comparison, the paper provides a comprehensive overview of the suitability of various consensus mechanisms within IoT-oriented distributed ledger systems.

Author: PODGÓRSKI, Paweł (Warsaw University of Technology, Faculty of Electrical Engineering)

Presenter: PODGÓRSKI, Paweł (Warsaw University of Technology, Faculty of Electrical Engineering)

Session Classification: Session C (Poster)

Contribution ID: **57** Type: **Poster**

Comparison of the Performance and Effectiveness of Hashing Algorithms

Thursday 24 April 2025 11:30 (30 minutes)

\documentclass[conference]{IEEEtran}
\usepackage[T1]{fontenc}
\usepackage{lscape}
\IEEEoverridecommandlockouts
% The preceding line is only needed to identify funding in the first footnote. If that is unneeded, please comment it out.
\usepackage{cite}
\usepackage{amsmath,amssymb,amsfonts}
\usepackage{algorithmic}
\usepackage{graphicx}
\usepackage{textcomp}
\usepackage{xcolor}
\def\BibTeX{{\rm B\kern-.05em{\sc i\kern-.025em b}\kern-.08em
T\kern-.1667em\lower.7ex\hbox{E}\kern-.125emX}}
\begin{document}

\title{Comparison of the Performance and Effectiveness of Hashing Algorithms\\
}

\author{\IEEEauthorblockN{1st Konrad Žilinski}
\IEEEauthorblockA{\textit{Institute of Theory of Electrical Engineering, Measurement and Information Systems} \\
\textit{Faculty of Electrical Engineering}\\
Pl. Politechniki 1, 00-661 Warsaw, Poland \\
konrad.zilinski.stud@pw.edu.pl}
}

\maketitle

\begin{abstract}
This study compares the performance and efficiency of various hashing algorithms with a focus on their collision resistance and computational speed. The study was conducted on a mobile platform, analyzing historical and modern implementations of hash functions such as MD5, SHA-1, SHA-2, SHA-3, and Blake in different variants. The paper discusses their applications, advantages, and disadvantages, as well as the impact of architecture on performance. The results of the tests made it possible to identify the algorithm that offers the optimal compromise between security and computational efficiency.
\end{abstract}

\begin{IEEEkeywords}
hashing functions, hash collision, mobile platform, performance
\end{IEEEkeywords}

\section{Introduction}
Hash functions are used every day in most of the world's electronic devices. They are an indispensable part of cryptography, structures, and checksums. The following discusses the concept of hash functions and their use.

\subsection{Hash function, what it is? }
A hash function is a set of actions that unidirectionally transforms input data into output data of a

certain length. An important aspect of such a function is, as mentioned earlier, the unidirectionality of the transformations. This means that the output data does not offer any information about the content of the input data.
No less important for a mixing function is its sensitivity to changes in the input data. Although an ideal hash function should generate a different result with a change as small as one bit, it should also generate a completely unique result for each unique file.

\subsection{Where are they used?}
The simplest application of the hash function is indexing. It involves assigning a unique ID to any type of data. When we need to arrange voluminous data in a structured way, it is inefficient and inconvenient to operate on entire files. Instead, the standard is to use mixing functions to assign unique strings of bits representing individual files. Thus, operations such as searches are greatly sped up because they use short strings.
Another realm in which hash functions are used is checksums. A hash function always produces the same result for the same input data. This property is used to confirm the immutability of the file. The result of the hash function is sent along with the file, and when it is received, another checksum is counted. If both checksums match, it means that the file has not been altered in any way.
However, the last but not least important application is cryptography. Hash functions are used for many different purposes. One of them is to make memorized passwords obfuscated. Instead of keeping passwords in the database, they are converted into the results of mixing functions. This ensures that passwords will not be disclosed during a potential data leak.

\section{Scope of the study}

No hash function is perfect. Each set of instructions compromises the speed of operation and quality of the result. In this study, I focused on the cryptographic part of hash functions. Their most important feature is resistance to result collisions, but this is not the only metric that will help us measure the performance of different functions.
A mobile platform was chosen to perform the study. The choice was based on several factors. First, mobile devices are widely available. The constant pursuit of the latest models causes us to accumulate many phones that are still fully operational. From this, the next reason for choice also arises - the historical aspect. This will allow us to compare the changes in trends in optimizing individual components.

\section{Tested functions}

\subsection {Message Digest (MD5)}
MD5 is the most popular mixing algorithm of the MD family. It was developed by Ron Rivers in 1991 as the successor to MD4. This algorithm generates hashes of 128 bits using the Merkle-Damgard architecture. However, the complexity of finding the collision of the result is not 2^{128} but 2^{18} \cite{b4}.

\subsection {Secure Hash Algorithm (SHA)}

\subsubsection {SHA-1}
In 1995, the National Institute of Standards and Technology (NIST) published a new hashing algorithm - SHA-1. Also, like MD5, it is based on the Merkle-Damgard architecture, and it only produces 160-bit hashes. And like its predecessors, it sweeps the ideal 2^{160} needed SHA-1 relies on at 2^{61} attempts.\cite{b4}

\subsubsection {SHA-2}
The next iteration of the Secure Hashing Algorithm hit the world in 2002. This time, the number of output bits is configurable, with 256, 384, and 512 bit variations available. SHA-2 is currently widely used, for example, in the Bitcoin cryptocurrency. However, like its predecessors using the Merkle-Damgard structure, hash collisions are increasingly common.

\subsubsection{SHA-3}
The next iteration of the Secure Mixing Algorithm hit the world in 2002. This time, the number of output bits is configurable, with 256, 384, and 512 bit variations available. SHA-2 is currently

widely used, for example, in the Bitcoin cryptocurrency. However, like its predecessors using the Merkle-Damgard structure, hash collisions are increasingly common.

\subsection {BLAKE}
BLAKE is one of the algorithms that competed for SHA-3. Based on the ChaCha encryption string, BLAKE has several iterations and variants. BLAKE2s is designed to run on 32-bit systems, while BLAKE2b runs on 64-bit systems. BLAKE3 is the latest iteration, improving the algorithm's performance.

\section{Devices used in the study}

```
\begin{table}[htbp]
\caption{Information about the devices used in the study}
\begin{center}
\begin{tabular}{|c|p{0.16\linewidth}|c|p{0.11\linewidth}|c|}
\hline
\textbf{Manufacturer} & \textbf{Model Name}& \textbf{Model}& \textbf{Android version} & \textbf{Premier}\\
\hline\hline
Samsung & Galaxy A5 & SM-A500FU & 6.0.1 & 2014 Q4 \\
\hline
Samsung & Galaxy Tab A 7.0 & SM-T280 & 5.1.1 & 2016 Q1 \\
\hline
Sony & Xperia XZ Premium & G8141 & 9 & 2017 Q1 \\
\hline
Xiaomi & Mi A1 & Mi A1 & 9 & 2017 Q3 \\
\hline
Samsung & Galaxy S10e & SM-G970F & 12 & 2019 Q1 \\
\hline
Samsung & Galaxy A21s & SM-A217F & 12 & 2020 Q1 \\
\hline
Sony & Xperia 1 IV & XQ-CT54 & 14 & 2022 Q2 \\
\hline
Samsung & Galaxy A54 & SM-A546B & 14 & 2023 Q1 \\
\hline
\end{tabular}
\label{tab1}
\end{center}
\end{table}

\begin{table}[htbp]
\caption{Technical information about the devices used in the study}
\begin{center}
\begin{tabular}{|p{0.16\linewidth}|p{0.13\linewidth}|p{0.14\linewidth}|p{0.36\linewidth}|}
\hline
\textbf{Model Name}& \textbf{RAM} & \textbf{Chipset}& \textbf{CPU} \\
\hline\hline
Galaxy A5 & 2GB LPDDR3 & Snapdragon 410 & 4x Cortex-A53 1190MHz \\
\hline
Galaxy Tab A 7.0 & 1.5GB LPDDR3 & Spreadtrum SC7730S & 4x Cortex-A7 1300MHz \\
\hline
Xperia XZ Premium & 4GB LPDDR4X & Snapdragon 835 & 4x Qualcomm Kryo 280LP 1900MHz,
\newline 4x Qualcomm Kryo 280HP 2457MHz \\
\hline
Mi A1 & 4GB LPDDR3 & Snapdragon 625 & 8x Cortex-A53 2016MHz \\
\hline
Galaxy S10e & 6GB LPDDR4X & Samsung Exynos 9820 & 2x Mongoose M4 2730MHz,\newline 2x
Cortex-A75 2310MHz,\newline 4x Cortex-A55 1950MHz \\
\hline
```

Galaxy A21s & 3GB LPDDR4X & Samsung Exynos 850 & 8x Cortex-A55 2002MHz \\
\hline
Xperia 1 IV & 12GB LPDDR5 & Snapdragon 8 Gen 1 & 4x Cortex-A510 1785MHz, \newline 3x Cortex-A710 2495MHz, \newline Cortex-X2 2995MHz \\
\hline
Galaxy A54 & 8GB LPDDR4X & Samsung Exynos 1380 & 4x Cortex-A55 2002MHz, \newline4x Cortex-A78 2400MHz \\
\hline
\end{tabular}
\label{tab1}
\end{center}
\end{table}

Tables 1 and 2 show all the information about devices used in the study. These devices are from 3 companies: SONY, SAMSUNG, and XIAOMI. The oldest tested phone premiered more than 11 years ago. While the newest - barely 2. All these phones are from different price shelves, from budget variants to flagship models.

\section{The application used to conduct the study}

Virtually every device uses a different version of Android, so a key aspect of the study was to choose a solution that would allow a comparison of all devices across 10 years of development. The first idea was to use the Termux application, allowing a .jar file to run. However, it was not possible to provide the same version of Java for all devices, more specifically, the oldest ones. The logical next step was to abandon running the files directly and create an entire mobile application. This is a simple application created using Android Studio. As you can see in "Fig.~\ref{rys:applikacja}", it takes 3 buttons. 1 - start the calculation, 2 - start the calculation in reverse order, and 3 - export the results to a .csv file. The calculation phase is started with a warm-up round, which greatly improves the consistency of results between runs. Then, 100 executions of mixing functions are divided into the available number of device cores. A data buffer is created for each new mixing function execution and for each data size. Time is measured only from the start of hashing to the receipt of output data.

\begin{figure}[htbp]
\centerline{\includegraphics[width=0.9\linewidth]{images/screenshot.png}}
\caption{Application screenshot}
\label{rys:applikacja}
\end{figure}

\section{Course of the study}

The first step of the study was to prepare the devices. Each device was charged and rebooted, excess files in memory were removed, and also airplane mode was turned on. Before each app launch, I made sure the device had a battery level above 40 and also that it was not hot. As part of the test, the app was run 3 times, twice forward and once backward, to average out any variation caused by device heating. Also, during the test, the device's display was periodically activated so that the phone did not fall into sleep mode. After each activation, the data was saved in the device's memory and then copied to a computer for analysis.

\section{Results}

\subsection{Simplest comparison}
The most obvious comparison that can be made is to create a time diagram of all calculations for a particular device. An example of a diagram from a Xiaomi Mi A1 device can be seen in "Fig.~\ref{rys:wykresGlownyXiaomi}". It clearly shows that the fastest functions are SHA-1 and SHA-256. Next comes MD5, and right behind it are SHA-512 and SHA-384. Next, algorithms from the SHA3 series are ordered. The tables are closed with algorithms from the BLAKE2 and BLAKE3 series.

\begin{figure}[!hb]

\centerline{\includegraphics[width=0.9\linewidth]{images/xiaomi.png}}
\caption{Average calculation time for Xiaomi Mi A1}
\label{rys:wykresGlownyXiaomi}
\end{figure}

\subsection{Historical context}

The obvious next comparison is to add historical context. "Fig.˜\ref{rys:zmiennoscWCzasie}" compares the computation time of 3 hashing functions (MD5, SHA1, and BLAKE2b) for two input data lengths(32MB and 32KB) on all devices. First, of course, all calculations on 32KB are faster than 32MB. Next, surprisingly, the MD5 is the fastest only on Samsung's oldest device. It is also interesting to note that a device 2 years younger (Samsung Tab A) is significantly faster at calculating SHA-3 and BLAKE2b but slower at calculating SHA1 and MD5. One more thing to mention is the distinct separation between premium models and budget ones. All prices models have multi architectural CPUs that allow the to excel in specific areas, On older Samsung phone from 2019 it can be observed particularly well as SHA3 caclucaltions were significantly decreased in time more than SHA1.

\begin{figure}[!hb]
\centerline{\includegraphics[width=0.9\linewidth]{images/zmiennoscWCzasie.png}}
\caption{Time comparison for particular hash functions for different devices}
\label{rys:zmiennoscWCzasie}
\end{figure}

\subsection{Moores Law}

Fig.˜\ref{rys:zmiennoscWCzasie}" shows that Moore's law is not preserved. The time required to calculate the hash function does not decrease twice yearly.Fig.˜\ref{rys:newvsold}" shows the acceleration for all types of functions. The average acceleration over 10 years is 14.6 times. This result was obtained by comparing the oldest mid-priced phone with the newest mid-priced phone from the same manufacturer, Samsung. Changing the price segment to premium, on the other hand, outlines significantly different values. The 5 years of development in this segment accelerates the performance by 20 percent alone.

\begin{figure}[!hb]
\centerline{\includegraphics[width=0.9\linewidth]{images/newvsold.png}}
\caption{Improvement comparison for different hash functions}
\label{rys:newvsold}
\end{figure}

\subsection{Comparison against the fastest function}

The previous diagrams show the execution time of various functions changing over the years. However, it illustrates not only the improvement of the algorithm but also the speeding up of the devices themselves.
On all devices except the oldest, the fastest hash function was the SHA-1 function.
It was chosen as the baseline.

\subsubsection{SHA-1 VS SHA-3}

Fig.˜\ref{rys:sha1vsSha3}" shows how much faster SHA-1 is compared to SHA-3. On the graph, we can identify 3 main groups. The slowest SHA-3 is on the oldest device, which is expected, but surprisingly, the second worst one is a phone from the year 2020. Next is a group of budget phones, and the last group is for the newest or premium phones. The most important part of this diagram is the results for the device premiered in 2017 Q3. This indicates that although this phone is one of the fastest (Fig.˜\ref{rys:zmiennoscWCzasie}"), its performance is not related to the acceleration of the SHA-3 algorithm but plain hardware improvement.

\begin{figure}[!hb]
\centerline{\includegraphics[width=0.9\linewidth]{images/sha1vssha3.png}}
\caption{SHA-1 vs SHA-3}

\label{rys:sha1vsSha3}
\end{figure}

\subsubsection{SHA-1 VS BLAKE}

Different BLAKE hashing algorithms have similar results. There are small differences that we were able to measure, from which it can be concluded that BLAKE in version 3 is the slowest one. Generally, BLAKE2b-256 is the best performer, but it is always slower than SHA-3, even compared to the 512-bit variant. Worth noting here is that 512-bit variants are marginally slower than their 256 versions, which indicates that these functions are not optimized for smaller sizes. BLAKE2s, which is meant for 32-bit devices, is also not optimized enough to make any significant impact - on devices that use 32-bit architecture, this algorithm matches the performance of BLAKE2b, and on all other devices, it performs worse. Comparison of BLAKE algorithms to SHA-1 is not much different from the SHA-3 situation: the worst performers are the oldest phone and the budget one.

\begin{figure}[!hb]
\centerline{\includegraphics[width=0.9\linewidth]{images/sha1vsBlake2b256.png}}
\caption{SHA-1 vs BLAKE2b-256}
\label{rys:sha1vssha3}
\end{figure}

\subsubsection{SHA-1 VS SHA-256}

SHA-256 also known as SHA2 is still widely used algorithm. Surprisingly, in the majority of devices, it performed very similarly to the deprecated SHA-1 algorithm, providing higher security. Based on "Fig.~\ref{rys:sha1vssha2}" it can be easily noted that SHA-1 performs up to 100\% better than SHA-256 on older phones. Subsequently, the newer the device, the better SHA-256 gets, matching or outperforming slightly SHA-1. Also, it is important to mention that differences here are measured in percentages because results are not bigger than twice the size. In contrast, differences with the BLAKE algorithm reached 60000\%.

\begin{figure}[!hb]
\centerline{\includegraphics[width=0.9\linewidth]{images/sha1vssha2.png}}
\caption{SHA-1 vs SHA-256}
\label{rys:sha1vssha2}
\end{figure}

\subsection{Collision resolution context}

All previous comparisons were based on measured time. Some hash functions were faster, some slower. As stated before, calculation speed is only one of the factors by which we can measure hash quality. An equally important aspect is also how collision-resistant the tested function is. To properly illustrate performance, taking into account both hashing time and offered collision resistance, equation \eqref{eq}" was developed. To aggregate further results, SHA-1 was once again used as a reference point, resulting in graphsFig.~\ref{rys:overallnew}" and "Fig.~\ref{rys:overallold}".

\begin{equation}
\frac{TrueCollisionResistance / MaxCollisionResistance}{TimeTaken} \label{eq}
\end{equation}

\begin{figure}[!hb]
\centerline{\includegraphics[width=0.9\linewidth]{images/finalold.png}}
\caption{Relative overall hash function performance for old device}
\label{rys:overallold}
\end{figure}

\begin{figure}[!hb]
\centerline{\includegraphics[width=0.9\linewidth]{images/finalnew.png}}
\caption{Relative overall hash function performance for newest device}
\label{rys:overallnew}
\end{figure}

Both of these graphs clearly indicate that the best performance is achieved by SHA-2 algorithms. It provides the biggest collision resistance quickest across all device generations. Comparing old and new devices, we also can conclude that the SHA-3 algorithm is catching up with the leader. It is close to outperforming SHA-384 and SHA-512. Second in line are BLAKE family algorithms. They provide similar collision resistance as SHA-3 but take significantly longer to calculate, resulting in lower performance. SHA-1 and MD5 did not make it onto the podium because of their lack of vulnerabilities. They are the fastest, but they also are not cryptographically viable.

\section{Overview}

The study comprehensively compared the performance and effectiveness of popular hashing algorithms across a diverse set of mobile devices spanning nearly a decade. It revealed that while older algorithms like MD5 and SHA-1 still demonstrate high speed, their lack of collision resistance renders them unsuitable for secure applications. Modern algorithms, especially SHA-2, strike the best balance between performance and cryptographic strength, maintaining high resistance to collisions with relatively fast processing times. Although SHA-3 and BLAKE series offer comparable security, their performance is notably dependent on device hardware and architecture, which limits their efficiency on budget or older devices. The findings confirm that algorithmic performance scales with both time and hardware capabilities, but not always proportionally, indicating that optimization plays a key role. Analysis proves that we should use tested methods like SHA-2 and not blindly use new and shiny ones, as paper studies \cite{b3} are sometimes far away from actual results.

\begin{thebibliography}{00}
\bibitem{b1} ALAMGIR, Nahiyan; NEJATI, Saeed; BRIGHT, Curtis. SHA-256 collision attack with programmatic SAT. arXiv preprint arXiv:2406.20072, 2024.
\bibitem{b2} GAURAVARAM, Praveen; MCCULLAGH, Adrian; DAWSON, Edward. Collision attacks on MD5 and SHA-1: Is this the "Sword of Damocles"for electronic commerce. Information Security Institue (ISI), Queensland University of Technology (QUT), Australia, 2006.
\bibitem{b3} BLACK, John; COCHRAN, Martin; HIGHLAND, Trevor. A study of the MD5 attacks: Insights and improvements. In: Fast Software Encryption: 13th International Workshop, FSE 2006, Graz, Austria, March 15-17, 2006, Revised Selected Papers 13. Springer Berlin Heidelberg, 2006. p. 262-277.
\bibitem{b4} MAETOUQ, Ali, et al. Comparison of hash function algorithms against attacks: A review. International Journal of Advanced Computer Science and Applications, 2018, 9.8.
\bibitem{b5} AUMASSON, Jean-Philippe, et al. BLAKE2: simpler, smaller, fast as MD5. In: International Conference on Applied Cryptography and Network Security. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013. p. 119-135.
\bibitem{b6} SASAKI, Yu, et al. Improved collision attack on MD5. Cryptology ePrint Archive, 2005.
\bibitem{b7} DEN BOER, Bert; BOSSELAERS, Antoon. Collisions for the compression function of MD5. In: Workshop on the Theory and Application of of Cryptographic Techniques. Berlin, Heidelberg: Springer Berlin Heidelberg, 1993. p. 293-304.

\end{thebibliography}
\vspace{12pt}

\end{document}

Author: ZILINSKI, Konrad

Presenter: ZILINSKI, Konrad

Session Classification: Session C (Poster)

Contribution ID: **58** Type: **Presentation**

Agent AI: współpraca, konkurencja czy symbioza?

Thursday 24 April 2025 09:10 (20 minutes)

Podróż przez ewolucję współpracy ludzi z AI, od pierwszych kroków do obecnych wyzwań. Jak będzie wyglądać ta relacja w przyszłości? Współpraca, rywalizacja, a może nowa symbioza?

Presenter: ADACH, Dawid

Session Classification: Keynote